Fratel

Réseau francophone de la régulation des télécommunications

QUELS DÉFIS POUR LA SÉCURITÉ DES RÉSEAUX DE NOUVELLE GÉNÉRATION ? SYNTHÈSE DU QUESTIONNAIRE ENVOYÉ AUX MEMBRES DU RÉSEAU

Brazzaville, 23 et 24 mai 2022

Définitions de résilience et sécurité

Il n'existe pas de définition commune de résilience ou de sécurité des réseaux

Résilience : capacité d'assurer la continuité des réseaux

- En général, la résilience d'un réseau de télécommunications est considérée comme la capacité des réseaux de communications électroniques à fournir sans interruption les services de télécommunications et à faire face à tout type de dysfonctionnements, de défaillances ou de menaces sur les réseaux
- La notion de rétablissement en cas de défaillance est évoquée par quelques pays

Sécurité : Notion qui inclut la cybersécurité pour plusieurs pays alors que pour d'autres, les deux termes sont synonymes

- La sécurité : résister à toute action (physique ou virtuelle) ou évènement volontaire ou non, qui compromettrait la disponibilité, l'authenticité, l'intégrité ou la confidentialité de ces réseaux ou services, des données stockées, transmises, ou traitées ou des services connexes offerts ou rendus accessibles par ces réseaux ou ces services.
- La cybersécurité : pratique consistant à protéger les réseaux, les systèmes et toute autre infrastructure numérique contre les attaques malveillantes
  - Mesures proactives et réactives visant à garantir la confidentialité, l'intégrité, la disponibilité, l'authenticité et la non-répudiation des informations sous forme électronique des ressources et services publics ou privés, dans le cyberespace

Mesures pour éviter la congestion des réseaux lors de la pandémie de Covid 19

Aucun pays membres de Fratel n'a subi de problèmes de congestion durant la pandémie

- Augmentation de trafic observée partout
- Réseaux suffisamment dimensionnés pour absorber ce pic
  - Dans certains pays, dimensionnement suffisant des réseaux du fait de la faible utilisation de l'internet mobile ou fixe

Mesures prises lors de la pandémie par les régulateurs

- coordination de crise avec les opérateurs nationaux (et internationaux) : surveillance de la disponibilité et la continuité des services, des appels d'urgence, de la qualité de service…
- accord pour diminuer le trafic sous la forme d'une diminution de la définition des images et vidéos avec des fournisseurs de contenus ou meures volontaires (niveau européen)
  - Mise à disposition les ressources de numérotation supplémentaires aux opérateurs qui ont fait la demande (Maurice) ou en fréquences (Guinée)
- guide de bonnes pratiques afin de sensibiliser les utilisateurs (France, Sénégal)

Leçons tirées par les régulateurs

- Peu de mesures spécifiques prises en lien avec la pandémie
- Mise en place d'un dialogue proactif entre les opérateurs et les principaux fournisseurs de contenu et d'applications pour anticiper des événements pouvant avoir un impact sur la charge des réseaux
- Nécessité d'interconnexion internationale accrue (Afrique centrale)
- fixation des indicateurs sur la surcharge des réseaux. (Sénégal)

Amélioration de la résilience des réseaux

Mesures ou protocoles pour répondre aux évènements extrêmes ou exceptionnels

- Plan national des télécommunications d'urgence (Belgique, Cameroun, Cap Vert, Côte d'Ivoire, Maurice,
  - Lignes directrices (ou directives) pour l'organisation et la mise en place des moyens de télécommunications nécessaires à la réponse aux catastrophes
- Obligations générales ou dans le cahier des charges des opérateurs
  - toute mesure pour assurer la permanence et disponibilité/accessibilité du service, plan de continuité de services relatif aux incidents graves, assurer la communication entre les services d'urgence et les autorités
- Pas de mesures spécifiques dans le cas particulier des enjeux climatiques
  - En Belgique, à la suite des inondations de 2021, différents groupes de travail ont été créés
  - Au Congo, Les infrastructures les plus vulnérables au climat sont celles de la transmission par faisceaux hertziens. Risque d'instabilité et d'indisponibilité des réseaux à cause des fortes pluies=> recommandations de l'ARPCE pour améliorer la résilience

Résilience et réseaux de nouvelle technologie

- Problèmes liés à la disponibilité des équipements et aux manques de puces électroniques
- Logiciels : points de défaillance unique
- Dépendance des opérateurs des points d'atterrissement des fibres optique transcontinentales
- Exploitation insuffisante des points d'échange internet (IPX)
- Risque de dilution des responsabilités avec la multiplicité des acteurs

Enjeux de sécurité des nouveaux réseaux (1/2)

Obligations des opérateurs de prendre toute mesure technique et organisationnelle pour limiter les risques

- Garantir un niveau de sécurité approprié au risque évalué et la continuité des services fournis
- Prescriptions techniques en matière de sécurité éventuellement édictées par le régulateur (Cameroun)
- Notification, dans les meilleurs délais, de toute atteinte à la sécurité ou perte d'intégrité ayant un impact significatif sur la fourniture des réseaux ou des services
  - Au régulateur (Roumanie, Sénégal), Ministre de l'Intérieur (France)

Enjeux de sécurité des nouveaux réseaux

- externalisation des infrastructures auprès d'une multiplicité d'acteurs (hyperscalers, Towercos, équipementiers)
- Virtualisation et programmation logicielle des réseaux => Sécurité « logicielle »
- Déport de l'intelligence et des traitements aux extrémités du réseau (edge computing)
- Protection des infrastructures critiques ;
- Protection des données personnelles, plus particulièrement liés aux technologies Cloud (hors du pays)
- Adoption des objets connectés (Internet des objets)
- Besoin de personnel compétent et surtout de formation du personnel

Enjeux de sécurité des nouveaux réseaux (2/2)

Mesures prises par les régulateurs pour assurer la sécurité des nouveaux réseaux

- Mise en œuvre de stratégies d'utilisation de plusieurs fournisseurs d'équipements de réseau dans les conditions d'appel à candidatures pour les fréquences 5G
- Dialogue avec les acteurs du marché
- Autorisation préalable des équipements - Homologation des équipements obligatoire dans certains pays (Côte d'Ivoire, Maurice, République de Guinée, République du Congo…)
- Technologies, équipements et logiciels dans les réseaux 5G développés par des fabricants autorisés (Roumanie)
- Formation du personnel

Obligations pour les opérateur OTT

- Obligations en matière de sécurité : Cadre européen
- Stratégie sous-régionale nécessaire selon l'ARPCE

Cybersécurité : compétences et mesures pour réduire les risques de cyberattaque

La cybersécurité hors des attributions de nombreux régulateurs télécoms

- Exceptions : Côte d'Ivoire, Belgique, Luxembourg
- Dans certains pays, création d'une agence en charge de la cybersécurité et/ou projet de stratégie nationale de cybersécurité en cours
- Contribution à la mise en place des textes législatifs et réglementaires
- Rôle de sensibilisation de la population (Ex. République du Congo)
- Contrôle du trafic notamment pour les appels internationaux entrant (Ex. Sénégal)
- Relations avec l'agence en charge de la cybersécurité en cas d'incident affectant la sécurité ou le fonctionnement des réseaux publics de communications électroniques (Ex. Roumanie)

Mise en place d'un CERT (« computer emergency response team ») et un CSIRT (« computer security incident response team ») au sein des autorités compétentes dans certains pays membres de Fratel

- Belgique, Bulgarie, Cameroun, Côte d'Ivoire, France, Luxembourg, Maurice, Roumanie, Suisse
- En cours de création au Cap Vert, Mali, Niger, Sénégal

Pays membres de FIRST (« Forum of incident reponse and security teams »)

- Belgique, Côte d'Ivoire, France, Luxembourg, Maurice, Roumanie, Suisse

Mesures pour réduire les risques de cyberattaque sont en général d'ordre réglementaire

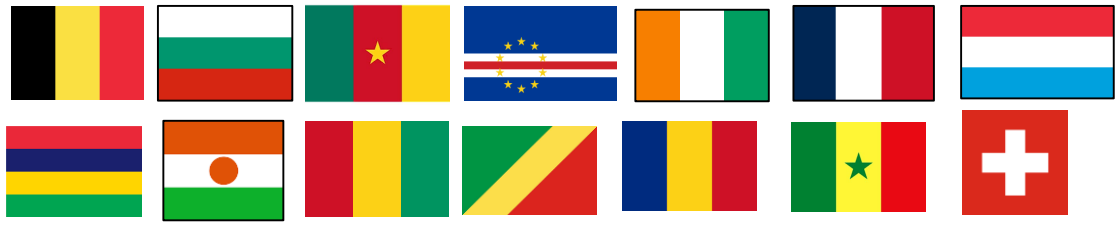
- Mise à disposition des opérateur par l'ILR d'un outil d'analyse de risque ainsi qu'une évaluation des mesures de sécurité proposé par l'ENISA

Audit des opérateurs sur la résilience et sécurité des réseaux

- Belgique, Bulgarie, Luxembourg, Cameroun, Cap Vert, Côte d'Ivoire, France, Roumanie
  - Conjointement avec l'autorité en charge de la cybersécurité au Cameroun
  - Décision revenant au Ministre chargé des communications électroniques en France

Merci aux 14 autorités membres du réseau qui ont répondu au questionnaire

- Belgique, Bulgarie, Cameroun, Cap Vert, Côte d'Ivoire, France, Luxembourg, Maurice, Niger, République de Guinée, République du Congo, Roumanie, Sénégal, Suisse



MERCI POUR VOTRE ATTENTION

Fratel
Réseau francophone de la régulation des télécommunications

Secrétariat exécutif de Fratel
Tél : +33 (0)1 40 47 72 28
Email : fratel@arcep.fr
www.fratel.org