Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC
Office fédéral de la communication OFCOM

Berne, le 16 novembre 2022

Modification de l'ordonnance sur les services de télécommunication (OST)

Sécurité des informations et des infrastructures et services de télécommunication

Rapport explicatif

Rapport explicatif

1 Contexte

La modification de l'art. 48a de la loi sur les télécommunications (LTC ; RS 784.10) est entrée en vigueur le 1er janvier 2021 (RO 2020 p. 6159). Elle donne au Conseil fédéral des compétences accrues dans le domaine de la sécurité de l'information et des infrastructures et services de télécommunications. Jusqu'à présent, le Conseil fédéral, sur la base de l'ancien art. 48a LTC (RO 2007 p. 921), ne réglait que l'annonce des perturbations des réseaux et des services de télécommunication (voir art. 96, al. 1, de l'ordonnance du 9 mars 2007 sur les services de télécommunication [OST ; RS 784.101.1]). Le présent projet de modification de l'OST vise à compléter cette dernière disposition par une première série de mesures destinées à préciser la réglementation relative à la notification des perturbations, à lutter contre la manipulation non autorisée d'installations de télécommunication au moyen de techniques de transmission des télécommunications et à garantir un haut niveau de sécurité dans l'exploitation à partir de la dernière génération de réseaux de radiocommunication mobile (réseaux 5G). Elle sera complétée par une autre série de mesures, dont des conséquences devront être analysées, notamment en vue d'assurer l'approvisionnement en électricité des réseaux de radiocommunication mobile.

1.1 Nécessité d'agir et objectifs

1.1.1 Sécurité des réseaux de radiocommunication mobile à partir de la 5e génération

Problématique

Selon l'Office fédéral de la statistique (OFS), en termes de nombre d'utilisateurs, l'Internet mobile en Suisse est passée de 43% en 2010 à 91% en 2019[1]. Dans le même temps, les réseaux mobiles se sont de plus en plus axés sur la technologie 5G. Selon Gartner, les investissements dans la 5G représentaient déjà 21.3 % des investissements consentis pour les infrastructures mobiles dans le monde en 2020[2]. Ericsson prévoit que la moitié du trafic mobile total passera par la 5G d'ici 2026[3]. Dans l'UE, les zones habitées devraient être entièrement couvertes par cette technologie d'ici 2030[4]. La 5G permettra aussi potentiellement des applications nouvelles ou améliorées dans des domaines sensibles comme la santé et l'énergie[5], et jouera un rôle central pour l'Internet des objets[6]. En outre, la radiocommunication mobile fait partie de l'infrastructure critique de la télécommunication, dont dépendent d'autres sous-secteurs critiques[7]. Il est donc important de garantir la sécurité des réseaux 5G et des prochaines générations.

Avec la diffusion croissante de la 5G, les questions de sécurité ont également gagné en importance dans le débat de politique étrangère. Le Département d'Etat américain considère que la sécurisation de cette technologie revêt une importance capitale[8]. Dans l'UE, une analyse des risques liés à la 5G a été réalisée en 2019, qui s'appuie elle-même sur les analyses des pays membres[9]. Elle montre que la disponibilité, la confidentialité et l'intégrité des données transmises via la 5G peuvent être mises en péril par différents acteurs (notamment des hackers, des organisations criminelles, des organisations étatiques ou soutenues par un Etat). Les fonctions du réseau central et la gestion des fonctions de réseau virtualisées sont particulièrement importantes pour garantir la sécurité. La 5G est au centre de l'attention car c'est la technologie la plus pertinente pour l'avenir par rapport aux réseaux de génération précédente. Les scénarios de risque identifient

1 Office fédéral de la statistique (2020): *Utilisation mobile d'internet,* https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/haushalte-bevoelkerung/mobile-internetnutzung.html.
2 Gartner (2020): *Gartner Says Worldwide 5G Network Infrastructure Spending to Almost Double in 2020,* https://www.gartner.com/en/newsroom/press-releases/gartner-says-worldwide-5g-network-infrastructure-spending-to-almost-double-in-2020.
3 Ericsson (2020): *More than 1 billion people will have access to 5G coverage by the end of 2020*, https://www.ericsson.com/en/press-releases/2020/11/more-than-1-billion-people-will-have-access-to-5g-coverage-by-the-end-of-2020.
4 Commission européenne (2021): *5G,* https://digital-strategy.ec.europa.eu/en/policies/5g.
5 OFCOM (2020): *Communications mobiles: évolution vers la 5G,* https://www.bakom.admin.ch/bakom/de/home/telekommunikation/technologie/5g.html.
6 Oracle (2019). *How 5G Networking Will Unleash the Full Potential of IoT*, https://blogs.oracle.com/scm/how-5g-networking-will-unleash-the-full-potential-of-iot-v2.
7 OFPP (2010). *Télécommunications,* https://www.babs.admin.ch/de/aufgabenbabs/ski/kritisch.html.
8 US State Department (2021): *Department Press Briefing*, https://www.state.gov/briefings/department-press-briefing-february-22-2021/.
9 NIS Cooperation Group (2019): *EU coordinated risk assessment of the cybersecurity of 5G networks*, https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

plusieurs situations critiques, par exemple lorsque les mesures de sécurité sont insuffisantes, que les appareils des utilisateurs finaux ne sont pas sécurisés ou que des fournisseurs sont mis sous pression par des acteurs menaçants.
Même si les scénarios de risque sont relativement peu probables, leurs conséquences seraient importantes, notamment en raison du rôle croissant de la 5G dans la téléphonie mobile. En outre, les scénarios décrits dans l'analyse des risques susmentionnée ne sont pas spécifiques à un pays et peuvent être transposés en Suisse. Toutefois, la Suisse se distingue par le fait que la base juridique actuelle ne permet qu'une action étatique limitée dans un avenir prévisible. A court terme, des mesures sont notamment possibles au niveau technique. Il faut également tenir compte du fait que les titulaires de concessions de radiocommunication mobile ont probablement aussi tout intérêt à garantir la sécurité de leurs réseaux 5G. Une enquête menée par l'OFCOM auprès des trois opérateurs suisses[10] montre également des activités importantes pour permettre des réseaux 5G sécurisés.

Objectif
L'objectif est de parvenir à un niveau minimum général de sécurité des réseaux 5G et des générations suivantes en Suisse, basé notamment sur les normes internationales.

1.1.2 Manipulation non autorisée d'installations de télécommunication

Problématique
Les cyberattaques causent des dommages économiques importants. Bien que les estimations varient considérablement, tous les experts reconnaissent que l'ampleur des dégâts se montent depuis longtemps en milliards de francs. En 2018, par exemple, l'Association Suisse d'Assurances (ASA) les a chiffrées à 9.5 milliards de francs[11] et il est probable que ce montant ait encore augmenté depuis. Les dommages touchent non seulement de grandes entreprises et des secteurs spécifiques, mais potentiellement toutes les entreprises[12], de même que des particuliers. Une enquête représentative menée auprès de dirigeants de PME a révélé que parmi les quelque 38'000 PME qui ont déjà été victimes d'une grave cyberattaque, une sur trois a subi un préjudice financier[13]. Si les cyberattaques ont de lourdes conséquences économiques, elles mettent également en danger la sécurité du pays, car elles peuvent provoquer des pannes ou perturber le fonctionnement des infrastructures critiques. Il y a donc un intérêt sécuritaire et économique à mettre en œuvre des mesures contre ce type d'attaques.
Les fournisseurs d'accès à Internet (FAI) jouent un rôle central dans la prévention des cyberattaques. Comme ils permettent à leurs clients de communiquer au moyen d'Internet et leur fournissent souvent directement l'équipement nécessaire, ils sont bien placés pour prendre des mesures préventives ou réactives qui ont un effet direct et qui sont d'une grande importance pour la cybersécurité de la Suisse. Sans une implication étroite des FAI, il ne sera pas possible de réduire de manière significative le nombre de cyberattaques. Etant donné que la menace de cyberattaques n'a cessé d'augmenter au cours des dernières années et que la tendance va vraisemblablement se poursuivre[14], l'adoption de mesures de protection devient d'autant plus urgente. L'Etat a le devoir d'examiner ces mesures. Il doit soutenir l'économie par le biais de points de contact et de centres de compétences et intensifier les poursuites pénales. Il doit également créer des cadres réglementaires pour une cybersécurité appropriée et les coordonner de manière appropriée. La définition des obligations incombant aux FAI constitue un instrument très important à cet égard. Rien ne sert d'introduire des mesures de protection strictes contre les cyberattaques dans différents secteurs économiques si, dans le même temps, le rôle des FAI dans ces efforts n'est pas défini.
Ces considérations ont conduit à réviser l'art. 48a de la LTC de telle sorte que les fournisseurs soient tenus de lutter contre les cyberattaques et "autorisés à dévier ou empêcher des communications et à supprimer

10 OFCOM (2021): *Enquête sur la 5G Toolbox (réponses confidentielles)*.
11 r i="on"> Association Suisse d'Assurances (2018): *Document de principe de l'ASA sur les cyberrisques*, https://www.svv.ch/sites/default/files/2018-04/Grundlagenpapier%20CyberRisiken_DE.pdf.
12 Selon l'Office fédéral de la statistique (2021): *Infrastructure TIC dans les entreprises*, https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/unternehmen/ikt-infrastruktur.assetdetail.17784535.html verfügen 100% der Schweizer Unternehmen über einen Internetanschluss.
13 Gfs-Zurich (2020): *Numérisation et cybersécurité dans les petites entreprises suisses*, https://kmu-transformation.ch/wp/wp-content/uploads/2020/12/Schlussbericht_Studienergebnisse_Digitalisierung_Transformation_Homeoffice_Cybersicherheit_KMU_2020_12.pdf.
14 Voir l'évaluation des tendances réalisée par le Forum économique mondial (WEF) en coopération avec l'université d'Oxford (2020): *Cybersecurity, emerging technology and systemic risk*, http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf.

des informations". Toutefois, la LTC ne précise pas les mesures spécifiques que les fournisseurs sont tenus de prendre pour se protéger contre les cyberattaques. Les mesures actuelles dans l'ordonnance sur les services de télécommunication ont été élaborées sous la houlette de l'OFCOM, en collaboration avec le Centre national pour la cybersécurité (NCSC).

Objectif
La proposition réglementaire concerne principalement la mise en œuvre et la concrétisation de l'action de l'Etat déjà prévue dans la LTC partiellement révisée. Les mesures servent à mettre en œuvre la LTC dans le but d'établir des règles uniformes et claires pour les différents FAI suisses. Ces règles devraient contribuer à accroître le niveau général de protection dans le domaine de la cybersécurité.

1.2 Options étudiées et solution retenue

1.2.1 Annonces de perturbations

Les fournisseurs de services de télécommunication (FST) sont tenus de signaler immédiatement à la Centrale nationale d'alarme toute perturbation dans l'exploitation de leurs installations et services de télécommunication qui peut toucher au moins 10'000 clients, et de publier des informations à ce sujet sur un site Internet librement accessible. L'obligation de signaler les perturbations sera désormais assurée conjointement par l'OFCOM et la Centrale nationale d'alarme (CENAL). Des synergies peuvent être exploitées en impliquant la CENAL, spécialisée dans les événements extraordinaires[15]. En outre, il existait déjà une réglementation comparable sur les signalements de perturbations à l'art. 96 OST, par exemple en ce qui concerne le seuil de notification dans les prescriptions techniques et administratives de l'OFCOM (SR 784.101.113/1.8). Ainsi, au niveau de l'ordonnance, les fournisseurs de services de télécommunication n'encourent pas de coûts supplémentaires importants par rapport au statu quo. C'est pourquoi les conséquences de cette mesure ne sont pas abordées plus en détail ci-après.
Le maintien du statu quo avec 30'00 clients concernés a été rejeté. La majorité des participants à la consultation publique ont demandé un seuil de notification plus bas.

1.2.2 Sécurité des réseaux mobiles à partir de la 5e génération

Voici les points essentiels des mesures contenues dans le projet de loi concernant la sécurité des réseaux mobiles:

- Les concessionnaires de radiocommunication mobile sont tenus d'exploiter un système de gestion de la sécurité de l'information (SGSI) conformément aux normes reconnues. Le système couvre également les plans de résilience et de continuité et réglemente le traitement des incidents de sécurité.
- Les concessionnaires de radiocommunication mobile sont tenus d'exploiter uniquement des installations critiques du point de vue de la sécurité, qui répondent aux normes reconnues. Une certification n'est pas obligatoire. Les fournisseurs de services de télécommunication doivent cependant assumer la responsabilité de veiller à ce que les installations répondent aux normes de sécurité reconnues.
- Les concessionnaires de radiocommunication mobile sont tenus d'exploiter leurs centres des opérations du réseau (Network Operations Centres) et leurs centres de gestion de la sécurité (Security Operations Centres) exclusivement dans les Etats dont la législation garantit une protection adéquate des données.
- Lorsque l'OFCOM soupçonne une violation du droit et qu'un soutien externe est nécessaire, il peut exiger des concessionnaires de radiocommunication mobile qu'ils se soumettent à un audit à leurs frais ou fassent tester par un organisme qualifié les installations de télécommunication concernées.

[15] Voir CENAL [2021]: La CENAL, https://www.naz.ch/naz/index

Un maintien du statu quo a été rejeté afin de déterminer, compte tenu de l'importance accrue de la radiocommunication mobile et de l'expansion rapide de la 5G[16], un niveau minimum de sécurité des réseaux général et contraignant pour la Suisse.
Les mesures de la Toolbox 5G[17] visant à réduire encore les risques dans la chaîne logistique des entreprises de radiocommunication mobile (p. ex., l'exclusion des fournisseurs à haut risque ou les exigences de diversification des fournisseurs), qui font partie des mesures dites stratégiques, n'ont pas été prises en compte. La loi sur les télécommunications ne fournit pas la base juridique nécessaire.
Les mesures de la Toolbox 5G reposent également en partie sur des instruments prévus dans des bases légales inexistantes en Suisse et qui ne sont pas spécifiques aux télécommunications, comme le mécanisme de filtrage des investissements directs étrangers, entré pleinement en vigueur dans l'UE en 2020[18].
Des mesures visant à mieux protéger les réseaux de radiocommunication mobile[19] contre les pannes de courant dans des situations particulières ou extraordinaires, ainsi que des mesures neutres sur le plan technologique destinées à accroître la sécurité des réseaux aussi en dehors de la 5G et des générations suivantes, sont actuellement examinées en profondeur et pourraient être intégrées dans un futur projet de loi.

1.2.3 Manipulation non autorisée d'installations de télécommunication

Pour examiner d'autres moyens d'action, il est important de garder à l'esprit que la marge de manœuvre est déterminée par la LTC partiellement révisée. Dans le message relatif à la révision partielle de la LTC du 6 septembre 2017[20], le Conseil fédéral a déjà esquissé cette marge de manœuvre. Il a précisé que l'obligation de lutter contre toute manipulation non autorisée d'installations de télécommunication par des transmissions au moyen de techniques de télécommunication, visait, par exemple, à prévenir la diffusion de logiciels malveillants et à bloquer des attaques contre la disponibilité des services Internet (attaques DDoS), mais pas l'accès physique ni la prévention de l'accès (*backdoors)* à un ordinateur ou à un logiciel.
La proposition de modification de l'OST correspond donc à l'intention exprimée dans le message. Les mesures et les raisons de les introduire sont présentées dans les chapitres suivants.

1.2.3.1 Mesure 1: Droit de bloquer ou de restreindre les accès à Internet et les ressources d'adressage, et obligation d'informer les clients

L'art. 48a LTC donne aux fournisseurs le droit de bloquer les accès à Internet ou d'en restreindre l'utilisation si cela est nécessaire pour protéger les installations. Ce droit s'applique seulement tant que le danger persiste. Dans ce cas, en vertu de l'ordonnance, les fournisseurs ont l'obligation d'informer leurs clients du blocage. Cette obligation sert à assurer la transparence vis-à-vis des utilisateurs et contribue à leur faire mieux comprendre la question de la sécurité et les mesures nécessaires.

1.2.3.2 Mesure 2: Obligation pour les fournisseurs de filtrer les paquets IP dont l'adresse IP source est falsifiée (spoofing)

Les paquets IP envoyés avec de fausses adresses IP sources sont les principaux déclencheurs des attaques contre la disponibilité des services web (attaques DDoS). Ces attaques sont encore très fréquentes et provoquent de gros dégâts. Les spécialistes de la sécurité chez NetScout ont identifié globalement plus de 10 millions d'attaques DDoS pour l'année 2020[21]. Les coûts de ces attaques sont très difficiles à estimer, car ils dépendent fortement de l'importance des services web pour les activités commerciales d'une entreprise, mais il est clair qu'ils peuvent avoir de graves conséquences financières pour les victimes. En outre, si les attaques touchent la disponibilité des infrastructures critiques, les conséquences peuvent aller bien au-

16 La progression du déploiement de la 5G peut être suivie sous: OFCOM (2021): *Emplacements des antennes,* http://map.funksender.admin.ch ainsi que sous OFCOM, Fréquences et antennes et Emplacement des stations émettrices (2021): *Atlas de la large bande*, https://map.geo.admin.ch/?topic=nga.
17 NIS Cooperation Group (2020): *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.
18 UE (2019): *Screening of foreign direct investment*, http://trade.ec.europa.eu/doclib/press/index.cfm?id=2006.
19 Conseil fédéral (2020): *Meilleure protection des réseaux de communication mobile contre les pannes d'électricité*, https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-81445.html.
20 Conseil fédéral (2017): *Message concernant la révision de la loi sur les télécommunications,* https://www.fedlex.admin.ch/eli/fga/2017/1933/de.
21 Netscout (2021): *Crossing the 10 Million Mark: DDoS Attacks in 2020*, https://www.netscout.com/blog/asert/crossing-10-million-mark-ddos-attacks-2020.

delà des dommages financiers. Dans le cas des hôpitaux ou des entreprises d'approvisionnement en énergie, par exemple, la vie et l'intégrité physique peuvent être menacées.
Des possibilités techniques de filtrage des adresses IP sources falsifiées permettent depuis des années de rendre les attaques DDoS beaucoup plus difficiles[22]. Toutefois, elles sont trop peu exploitées[23], peut-être par manque d'incitations économiques[24]. Les fournisseurs supportent des coûts lors de la mise en place du filtrage, mais l'effet protecteur ne peut être internalisé (il consiste à rendre les attaques DDoS généralement plus difficiles à réaliser)[25]. Il y a donc un problème classique de "bien commun", même s'il est atténué par le fait que les coûts de mise en place des filtres ont tendance à diminuer[26]. L'introduction d'une obligation générale de filtrage pourrait désamorcer ce problème; dans ce cas, tous les fournisseurs contribueraient à rendre plus difficile la réalisation d'attaques DDoS.

1.2.3.3 Mesure 3: Obligation pour les fournisseurs de configurer de manière sûre les terminaux mis à la disposition des clients

En raison de leur utilisation très répandue, les appareils et équipements terminaux remis par les fournisseurs à leurs clients jouent un rôle majeur dans la cybersécurité. S'ils présentent des vulnérabilités généralisées, les pirates peuvent accéder à des milliers d'appareils et utiliser leur puissance de traitement pour mener des attaques, par exemple des attaques DDoS[27]. Les routeurs, qui sont livrés avec des mots de passe par défaut, constituent un exemple classique de ce problème. La question de la configuration sécurisée des terminaux devient encore plus importante avec la multiplication très rapide des appareils connectés de l'Internet des objets[28]. Si les terminaux ne sont pas configurés de manière sécurisée, les pirates peuvent les manipuler très facilement pour ensuite exploiter leur puissance de traitement[29].
Une obligation légale pour les fournisseurs de configurer les terminaux de manière sécurisée est nécessaire, car les coûts du manque de sécurité ne seraient pas supportés par la collectivité, mais par ceux qui distribuent des appareils. Les fournisseurs souhaitent obtenir les coûts les plus bas possibles pour l'achat et la livraison des appareils. Or, les prescriptions de sécurité peuvent augmenter les prix. Afin que les fournisseurs qui attachent une grande importance à la sécurité ne soient pas pénalisés par le marché, il est nécessaire de fixer des exigences minimales applicables à tous. La réglementation correspond à l'intention du Conseil fédéral, exprimée dans son rapport en réponse au Po. 17.4295 Glättli, de soutenir l'application des normes de sécurité des appareils IoT par le biais de mesures et de réglementations étatiques[30].

1.2.3.4 Mesure 4: Obligation pour les fournisseurs d'exploiter un service spécialisé pour la notification des manipulations et de prendre des mesures de défense

La cybersécurité ne peut être améliorée que si les autorités nationales et internationales, les organismes spécialisés et les fournisseurs d'accès à Internet coopèrent activement. Comme les acteurs sont nombreux, il est important que les points de contact soient gérés de manière standardisée. C'est pourquoi les fournisseurs sont tenus de mettre en place un service de signalement (*abuse desk*) et d'établir un contact avec le registre Internet régional (RIR)[31] compétent. Il appartient aux fournisseurs de gérer eux-mêmes ce service ou de déléguer cette tâche à des tiers.
Comme un accès manipulé met en danger la sécurité de nombreux autres utilisateurs, il est très important de réagir rapidement. Les FAI doivent donc prendre des mesures dans un délai raisonnable. La menace ne

22 Lone et al. (2020): *SAVing the Internet: Explaining the Adoption of Source Address Validation by Internet Service Providers*, https://weis2020.econinfosec.org/wp-content/uploads/sites/8/2020/06/weis20-final31.pdf.
23 Luckie et al. (2019): *Network hygiene, incentives, and regulation: Deployment of source address validation in the internet*, https://researchcommons.waikato.ac.nz/handle/10289/13176.
24 Bauer et Eeten (2009): *Cybersecurity: Stakeholder incentives, externalities, and policy options,* https://www.researchgate.net/publication/227426674_Cybersecurity_Stakeholder_incentives_externalities_and_policy_options.
25 Christin (2011): *Network Security Games: Combining Game Theory, Behavioral Economics, and Network Measurements,* https://link.springer.com/chapter/10.1007/978-3-642-25280-8_2.
26 McConachie (2014): *Anti-Spoofing, BCP 38, and the Tragedy of the Commons,* https://www.circleid.com/posts/20140801_anti_spoofing_bcp_38_and_the_tragedy_of_the_commons/.
27 Vixie et al. (2014): *Abuse of Customer Premise Equipment and Recommended Actions*, https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=312647.
28 Vlajic et Zhou (2018): *IoT as a Land of Opportunity for DDoS Hackers*, https://ieeexplore.ieee.org/abstract/document/8423144.
29 Le cas le plus marquant est le botnet Mirai, qui, à son apogée en 2016, comprenait jusqu'à 500'000 appareils IoT infectés et était utilisé pour des attaques DDoS très puissantes. Pour un aperçu général du rôle de l'IoT dans les attaques DDoS, voir Vingau, Khoury et Hallé (2019): *10 Years of IoT Malware: A Feature-Based Taxonomy,* https://ieeexplore.ieee.org/abstract/document/8859496.
30 Conseil fédéral (2020): *Normes de sécurité pour les appareils connectés à internet (internet des objets)*, https://www.efd.admin.ch/dam/efd/de/dokumente/home/dokumentation/berichte/internet-things.pdf.download.pdf/29042020%20Bericht%20IoT-d.pdf.
31 Iana (2021): *Number Resources*, https://www.iana.org/numbers.

pourra peut-être pas toujours être traitée dans ce délai, mais une réaction doit avoir été initiée.

1.2.3.5 Autres possibilités d'action

Comparée au statu quo, tel qu'inscrit dans la LTC révisée, la modification de l'OST introduit des précisions. Celles-ci correspondent aux intentions expliquées dans le message relatif à la révision de la LTC. Y renoncer ne supprimerait pas l'obligation à laquelle les fournisseurs sont soumis en vertu de l'art. 48*a* LTC, mais son sens resterait flou, ce qui créerait une incertitude juridique.
Comme alternative au statu quo, il y aurait notamment la possibilité de prévoir des mesures concrètes plus restrictives que celles décrites dans le projet. Selon ce dernier, les fournisseurs ne sont pas obligés de bloquer les accès à Internet ni les ressources d'adressage qui constituent une menace; ils en ont seulement le droit. Une obligation a été délibérément écartée, car les fournisseurs doivent continuer à pouvoir juger par eux-mêmes dans quels cas un blocage est nécessaire. Ils conservent ainsi la liberté de garantir la sécurité de leurs services avec les moyens qui leur conviennent le mieux. L'alternative serait que le blocage soit prescrit ou puisse être ordonné par les autorités. L'introduction d'une obligation pour les fournisseurs de protéger leurs clients contre les attaques DDoS[32] n'a pas été retenue non plus: pour cela, les fournisseurs devraient être en mesure d'absorber un volume de trafic beaucoup plus important que le trafic Internet habituel. Les instruments nécessaires sont relativement coûteux. En outre, une protection contre les attaques DDoS est déjà proposée sur le marché; les clients peuvent l'acquérir. Il n'est donc pas nécessaire d'exiger des fournisseurs qu'ils protègent tous leurs clients contre de telles attaques.

2 Présentation du projet

2.1 Réglementation proposée

La réglementation proposée prévoit une modification de l'art. 96 OST afin d'institutionnaliser la collaboration entre l'OFCOM et la Centrale nationale d'alarme dans la réception et le traitement des signalements de perturbations des réseaux et services de télécommunication. De nouvelles dispositions prévoient des mesures pour lutter contre la manipulation non autorisée d'installations de télécommunication par des transmissions au moyen de techniques de télécommunication et pour garantir la sécurité des réseaux mobiles à partir de la 5e génération.

2.2 Mise en œuvre

2.2.1 Sécurité des réseaux mobiles à partir de la 5e génération

Le projet se limite en grande partie aux mesures déjà mises en œuvre dans d'autres pays, notamment dans l'UE[33]. Ces mesures se basent partiellement sur des normes internationales (p. ex. 3GPP), auxquelles participe également l'industrie de la radiocommunication mobile[34]. S'agissant des audits prévus à l'art. 96*g*, leur but est de vérifier le respect des normes reconnues, ce pour quoi il existe également des processus établis.

2.2.2 Manipulation non autorisée d'installations de télécommunication

En ce qui concerne l'obligation faite aux fournisseurs d'accès à Internet d'informer les clients conformément à la mesure 1, il faut partir du principe qu'il existe des canaux de communication établis pour atteindre le client. Selon les explications données au point 1.2.3.1, l'obligation de filtrer les paquets IP dont l'adresse IP source est falsifiée (mesure 2) est une procédure éprouvée pour la mise en œuvre de laquelle les fournisseurs Internet peuvent, au besoin, se référer à des aides disponibles publiquement. En ce qui concerne l'obligation de configurer et d'entretenir correctement les terminaux (mesure 3), il devrait être possible, dans la plupart des cas, de s'appuyer sur les relations existantes avec les fournisseurs d'appareils et de les adapter si nécessaire. Dans le cas de la mesure 4, un fournisseur d'accès Internet ne doit intervenir que s'il est

32 Ceci contrairement aux mesures 1 et 2, par exemple, qui ne sont pas destinées à protéger spécifiquement les clients d'un FAI, mais à protéger de manière générale contre les attaques DDoS les destinataires du trafic Internet généré par les clients d'un FAI.
33 NIS Cooperation Group (2020): *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity,* https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity.
34 3GPP (2021). *Partners*, https://www.3gpp.org/about-3gpp/partners.

contacté par le NCSC. Il prend alors des mesures de défense dans un délai raisonnable.

3 Commentaire sur les dispositions

Les art. 96 et suivants sont répartis dans trois sections en fonction de leur champ d'application à raison des personnes. La section 3 (signalement de perturbations) concerne, comme aujourd'hui, tous les fournisseurs de services de télécommunication. Les dispositions sur la manipulation non autorisée d'installations de télécommunication (section 4) s'appliquent à tout fournisseur qui offre l'accès à Internet. Quant au cercle des personnes concernées par la section 5, il est restreint aux seuls concessionnaires de radiocommunication mobile, à savoir Salt, Sunrise UPC et Swisscom. A raison de la matière, les dispositions de la section 5 ne s'appliquent en outre qu'aux réseaux de radiocommunication mobile à partir de la cinquième génération (voir art. 96d).

Section 3 Signalement de perturbations (art. 96)

L'obligation pour les fournisseurs de services de télécommunication de signaler à l'OFCOM toute perturbation de l'exploitation de leur réseau a été introduite le 1er avril 2007, à l'art. 96 OST. Les détails de cette exigence sont réglés dans les prescriptions techniques et administratives de l'OFCOM concernant l'annonce des perturbations des réseaux (RS 784.101.113/1.8).
Les perturbations doivent être signalées à l'OFCOM au moyen d'un formulaire en ligne ou par courriel. Il existe également une solution de secours par téléphone. Les signalements sont traités pendant les heures de bureau et distribués aux organisations concernées.
Afin d'améliorer le traitement et la diffusion des signalements, il est prévu de coopérer avec la Centrale nationale d'alarme (CENAL), dont la réception de signalements est une des tâches essentielles. La CENAL dispose à cet effet d'une infrastructure informatique sécurisée qui fonctionne 24 heures sur 24. Elle sera en mesure de traiter et de distribuer les signalements de perturbations en temps réel, ce qui permettra d'accroître l'utilité des signalements, notamment dans la gestion de crise.
Aujourd'hui déjà, les fournisseurs de services de télécommunication transmettent partiellement des signalements de perturbations non seulement à l'OFCOM, mais aussi à la CENAL. La coopération prévue entre l'OFCOM et la CENAL éliminera ces doublons et simplifiera la procédure de signalement.
Pour concrétiser les considérations ci-dessus, l'art. 96 OST est complété de sorte que les perturbations doivent être signalées à la CENAL. L'OFCOM est pour sa part informé par la CENAL des perturbations signalées. Sur la base notamment des avis exprimés lors de la consultation et de l'audition sur les prescriptions techniques et administratives, la portée des perturbations, principal motif de l'obligation de signaler les perturbations, est abaissée à 10'000 clients. En outre, elle sera désormais réglée dans l'OST et non plus dans les prescriptions techniques et administratives.
Enfin, les fournisseurs de services de télécommunication ont désormais l'obligation de fournir, sur un site Internet librement accessible, des informations sur les perturbations, celles-ci constituant un élément d'évaluation de la qualité des services au sens de l'art. 12a, al. 2, LTC.

Section 4 Manipulation non autorisée d'installations de télécommunication

En introduction, il convient de noter que les dispositions contenues dans cette section ne sont applicables qu'aux fournisseurs d'accès à Internet car, de fait, ils sont les seuls à être concernés par les manipulations non autorisées d'installations de télécommunication.

Art. 96a Mesures de sécurité

Lorsque des installations de télécommunication sont infectées par un logiciel malveillant, elles risquent de mettre en danger les autres installations de télécommunication auxquelles elles peuvent se connecter. Le logiciel malveillant peut se propager via la connexion ou être utilisé pour d'autres activités nuisibles, comme l'envoi de spam, le phishing ou la participation à une attaque DDoS. Pour cette raison, il est nécessaire de prévoir, à l'al. 3, des mesures contre les installations de télécommunication infectées ou vulnérables. Différentes mesures sont envisageables. La connexion Internet peut être bloquée ou restreinte afin d'interrompre une activité nuisible. Elle peut l'être également si un appareil vulnérable est utilisé pendant une longue période, afin de protéger les autres abonnés ainsi que la personne ou l'entreprise touchée (mot-clé: attaques

par ransomware). Les appareils infectés peuvent aussi être placés dans un mode "sandbox" ("walled garden"), dans lequel le raccordement Internet vers le fournisseur de services de télécommunication est maintenu, mais la connexion Internet est fortement limitée ou carrément bloquée; ainsi, l'installation de télécommunication ne constitue plus une menace pour les autres. Si des activités nuisibles sont liées à des ressources d'adressage (adresses IP ou noms de domaine), celles-ci peuvent être bloquées pour l'accès clients. Dans la mesure où cela est techniquement possible, l'accès aux services d'urgence doit être exclu de ces mesures.
Lorsque des utilisateurs sont fortement touchés par des blocages et des restrictions de leur raccordement Internet, les fournisseurs d'accès à Internet doivent impérativement et rapidement les en informer. Ils doivent en outre les informer de manière transparente des mesures prises.
Les fournisseurs habilités à procéder au blocage ou à une restriction de l'utilisation en vertu de cette disposition devront renoncer aux mesures correspondantes ou du moins se mettre en relation avec le service Surveillance de la correspondance par poste et télécommunication (SCPT) s'ils savent que l'accès à Internet ou la ressource d'adressage en question fait l'objet d'un ordre de surveillance. Cette procédure découle déjà de l'art. 26, al. 2, let. a, de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT; RS 780.1) ainsi que de l'art. 29, al. 2 et 3, de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT; RS 780.11).
L'al. 2 de cette disposition réglemente la lutte contre les attaques visant à rendre les services Internet inaccessibles en générant un grand nombre de requêtes (attaques par déni de service ou *distributed denial-of-service attack* - DDoS). Ce cas est explicitement mentionné dans le message sur la révision de la LTC.
L'une des mesures consiste à empêcher l'utilisation de fausses adresses IP par les agresseurs (spoofing), ce qui rend impossible les attaques DDoS basées sur l'usurpation d'une adresse IP. Par conséquent, les fournisseurs d'accès à Internet sont tenus d'utiliser des mesures techniques raisonnables qui leur permettent de filtrer les paquets IP provenant de leur réseau avec une adresse IP source falsifiée. Pour mettre en place ces filtres, les fournisseurs doivent tenir à jour une liste des réseaux autorisés, laquelle peut être générée automatiquement à partir de la table de routage. Les étapes techniques nécessaires sont décrites par l'Internet Engineering Task Force (IETF) dans les "Best Current Practices" BCP38 pour les réseaux à hébergement unique (réseaux dans lesquels chaque appareil dispose d'une adresse IP) et BCP84 pour les réseaux à hébergement multiple (réseaux dans lesquels un appareil dispose de plusieurs adresses IP).
Les fournisseurs d'accès à Internet mettent souvent des terminaux à la disposition de leurs clients. En raison de leur utilisation très répandue, ceux-ci jouent un rôle important dans la lutte contre les cyberincidents. L'al. 3 prévoit donc que les caractéristiques de sécurité de toutes les installations de télécommunication qui sont mises à la disposition des clients doivent être configurées conformément aux règles techniques reconnues. Dans la mesure où les fournisseurs continuent d'exercer un contrôle technique sur ces installations, ils ont l'obligation de mettre à jour les installations de télécommunication correspondantes en temps utile. Cela permet de combler les failles de sécurité de ces appareils au moyen de mises à jour.
Pour les terminaux mobiles - qu'ils fonctionnent avec Android, iOS ou un autre système d'exploitation - c'est l'utilisateur qui décide si et quand le système d'exploitation doit être mis à jour. Les systèmes d'exploitation de ces terminaux ne sont pas considérés comme des installations de télécommunication relevant de l'influence et de la compétence d'un opérateur.
Il en va autrement des cartes SIM (ou eSIM) qui sont insérées dans de tels appareils. Elles ne peuvent être configurées ou mises à jour que par les opérateurs. Lors de la configuration, les règles de sécurité correspondant à l'état de la technique doivent en outre être respectées.
Si les mises à jour ne sont plus possibles et qu'il en résulte un risque pour la sécurité, les installations de télécommunication doivent être remplacées. L'OFCOM détermine quelles installations sont concernées et édicte les prescriptions techniques et administratives nécessaires afin de réduire au maximum l'exposition de ces appareils aux risques. Les principes suivants devront notamment être pris en compte:

- Aucune donnée d'accès standard (nom d'utilisateur, mot de passe) ne peut être utilisée pour accéder au terminal. Les données d'accès doivent être attribuées individuellement par appareil. Si cela n'est techniquement pas possible, un changement des données d'accès doit être imposé lors de la mise en service.
- Les services non utilisés sur le terminal doivent être désactivés par défaut.
- Le trafic SMTP sortant sur le port 25 doit être bloqué par défaut sur tous les raccordements de clients privés (raccordements "résidentiels", généralement des adresses IP dynamiques). En cas de besoin spécifique ou à la demande justifiée du client, il est envisageable de le débloquer.

- Par défaut, sur un terminal à l'état de livraison, aucun port librement accessible depuis Internet ne doit être ouvert. Les ports ouverts nécessaires au fonctionnement du terminal doivent être sécurisés par des mesures techniques (p. ex. restriction IP, liste de contrôle d'accès ou autres).
- Les ports utilisés pour la télémaintenance par le fournisseur doivent être limités autant que possible (p. ex., à un segment d'adresse IP utilisé par le fournisseur à cette fin).
- Le protocole utilisé pour l'accès à la maintenance à distance doit être protégé par une technologie de cryptage actuelle.
- Les mises à jour de sécurité classées comme critiques par le fabricant doivent être rapidement installées sur les terminaux. Si le fabricant n'effectue plus les mises à jour de sécurité sur les terminaux, ceux-ci doivent être remplacés.

Un délai de transition d'un an est prévu pour la mise en œuvre des al. 2 et 3.

Art. 96b Service de signalement

L'art. 96b prévoit que les fournisseurs d'accès à Internet disposent d'un service spécialisé (appelé abuse desk) pour le signalement des manipulation non autorisée d'installations de télécommunication par des transmissions au moyen de techniques de télécommunication (infections, piratages ou vulnérabilités des systèmes, attaques DDoS, spams, phishing, etc.). Ce service spécialisé du FAI a pour seule tâche de recueillir les signalements de manipulations non autorisées et de prendre de son propre chef les mesures de défense appropriées. Il appartient à l'entreprise de décider si, au sein de l'entreprise, c'est le service de signalement ou une autre personne qui est compétent pour prendre des mesures. L'obligation de prendre des mesures incombe à l'entreprise dans son ensemble. Elle n'a aucune obligation particulière de communiquer les signalements reçus à une quelconque autorité ou autre service spécialisé comme le NCSC, l'obligation des FAI de signaler étant réglée exclusivement par l'art. 96 OST. Les fournisseurs sont libres d'exploiter eux-mêmes ce service, qui peut être conçu en fonction de leurs besoins, ou d'en confier la gestion à des tiers. Le service de signalement peut être intégré dans les services d'annonces existants des FAI comme les «hotlines». Il convient toutefois de veiller à ce que des mesures de lutte appropriées puissent être engagées dans un délai raisonnable. En outre, les exigences techniques et administratives suivantes doivent être respectées:

- En principe, pour chaque intervalle réseau (blocs d'adresses IP), un contact (adresse électronique) doit être indiqué ("abuse-c") auprès du "registre Internet régional" (RIR) compétent. A défaut, les fournisseurs doivent donner un contact général pour les questions techniques ("tech-c"). Ils doivent s'assurer que ce contact peut remplir la fonction de service de signalement.
- Les fournisseurs veillent à ce que les manipulations puissent être signalées via l'adresse indiquée et à ce qu'il soit possible d'y réagir dans les délais impartis.
- Etant donné que les signalements de manipulations contiennent souvent des modèles qui sont triés par des filtres anti-spam, les éventuels filtres devraient être configurés très soigneusement et il faut s'assurer que le message est traité dans tous les cas.

Si la notion juridique de "dans un délai raisonnable" s'avère trop ouverte, l'OFCOM pourrait, le cas échéant, la préciser dans les prescriptions techniques et administratives, par exemple en prévoyant une durée spécifique et/ou en adoptant des règles différentes selon la catégorie de personnes qui font un signalement. Les mesures appropriées que peut prendre un fournisseur d'accès Internet ne se limitent pas au blocage des adresses IP et/ou d'autres ressources d'adressage, mais peuvent porter sur toute mesure jugée appropriée contre des manipulations non autorisée d'installations de télécommunication.

Art. 96c Exécution

L'OFCOM exécute la présente disposition et édicte les prescriptions techniques et administratives correspondantes. Le NCSC lui fournit l'expertise technique nécessaire.

Section 5 Sécurité des réseaux et des services exploités par les concessionnaires de radiocommunication mobile

Art. 96d Application

Toutes les dispositions concernant les fonctions de sécurité seront valables pour les réseaux 5G Stand Alone (selon les normes 5G 3GPP TS 33.501) et également pour les réseaux des technologies futures. En effet, les réseaux 5G actuels ne disposent pas d'un cœur de réseau 5G, ce sont des réseaux 5G Non Stand Alone dont les stations radio 5G sont actuellement exploitées sur l'infrastructure existante des réseaux 4G et non sur une infrastructure 5G complète (5G Stand Alone).
Les fonctions de sécurité 5G relatives au cryptage du trafic de données, à l'accès au réseau et à l'authentification (TS 33.501) normalisées par le 3GPP sont basées sur la sécurité 4G, c'est-à-dire que de nombreuses fonctions de sécurité 5G sont identiques aux fonctions de sécurité de la norme 4G.
Les nouvelles fonctions de sécurité ajoutées dans la 5G (par exemple, la protection contre l'usurpation d'identité du cœur de réseau, la protection du suivi des utilisateurs, l'authentification sans SIM des appareils IoT) reposent sur l'existence d'un cœur de réseau 5G (fonctions logiques pour gérer les nouveaux accès et le contrôle des stations radio 5G). Par conséquent, les fonctions de sécurité spécifiées dans la norme TS 33.501 qui vont au-delà de la 4G ne peuvent pas être techniquement mises en œuvre avant l'introduction de la 5G autonome (Stand Alone). Il semble cohérent de maintenir les mesures prises pour augmenter la sécurité également dans les réseaux des futures technologies.

Art. 96e Gestion de la sécurité

L'infrastructure de téléphonie mobile 5G ainsi que les infrastructures des futures technologies qu'elle génère et qu'elle traite sont des biens importants qui nécessitent d'être gérés de manière consciencieuse afin d'assurer la fiabilité et la disponibilité des services.
L'al. 1 impose dorénavant aux concessionnaires de radiocommunication mobile de développer, mettre en œuvre et de réexaminer continuellement un système de gestion de la sécurité de l'information (SGSI) à l'instar de ce que la plupart d'entre eux ont d'ores et déjà concrétisé.
La mise en œuvre d'un SGSI requiert une phase de planification durant laquelle les risques encourus par l'organisation concernée sont identifiés et évalués. Cette première phase permet de définir ensuite une politique de sécurité qui tient compte des risques à considérer, puis de décrire les objectifs à atteindre en matière de sécurité ainsi que le périmètre à sécuriser. Sur cette base, l'organisation déterminera finalement les contrôles correspondant à sa politique de sécurité et aux risques contre lesquels elle a choisi de se prémunir.
Pour le secteur des technologies de l'information et de la communication, des SGSI ont été développés sous forme de normes. Il s'agit notamment de la série de normes ISO/IEC 2700x (ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems – Requirements; ISO/IEC 27002:2005 Information technology – Code of pratice for Information Security Management; ISO/IEC 27011:2008 Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002) auxquelles il est prévu de se référer dans les prescriptions techniques et administratives en vertu de l'al. 96*g,* al.1.
Ces normes couvrent notamment les aspects de la sécurité physique, de la gestion des accès et de la sécurité des logiciels. Bien que la gestion de la continuité opérationnelle ainsi que la gestion des incidents de sécurité soient d'habitude également comprises dans des SGSI tels que ceux décrits dans les normes ISO/IEC 2700x, ces aspects sont tout de même mentionnés à l'al. 2 puisqu'il s'agit d'éléments qu'il convient impérativement de prendre en compte lorsqu'il s'agit de fournir des services au grand public. Pour préciser les exigences en matière de gestion de la continuité et des incidents, il est prévu de faire référence à la norme ISO 22301:2019 *Security and resilience — Business continuity management systems — Requirements* dans les prescriptions techniques et administratives.
Un SGSI s'adresse aux directions d'entreprise, aux collaborateurs responsables de la sécurité ainsi qu'à des évaluateurs externes. Une évaluation indépendante effectuée par un organisme de certification accrédité peut en effet conduire à une certification reconnue démontrant la capacité de la société en question à maîtriser la gestion de la sécurité. Il n'est pour l'heure pas prévu d'imposer une telle certification aux concessionnaires de radiocommunication mobile. Dans le cadre de la surveillance, l'OFCOM pourra toutefois exiger la remise, par le concessionnaire, d'informations relatives à la mise en œuvre du SGSI (voir art. 96g, al. 2).

L'élaboration d'un SGSI est influencée par les objectifs, les besoins, les exigences ainsi que les risques liés aux activités de l'organisation considérée. Elle dépend par ailleurs des technologies utilisées, de la clientèle, de même que de la grandeur et de la structure de l'organisation. Toute évolution de ces critères doit provoquer une adaptation du système de gestion de la sécurité. L'effort à consentir pour la mise en œuvre d'un SGSI est donc directement lié à l'organisation et aux services proposés.

Art. 96f Exploitation des installations de télécommunication critiques

Selon l'al. 1 de la présente disposition, les concessionnaires de radiocommunication mobile doivent garantir que les installations de télécommunication critiques du point de vue de la sécurité qu'ils exploitent correspondent à l'état de la technique. L'OFCOM peut définir les installations concernées, au besoin en collaboration avec la branche. La liste des installations critiques sera énumérée dans les prescriptions techniques et administratives correspondantes (art. 96*g*, al. 1).
Au niveau européen, et suite à une demande de la Commission Européenne, l'ENISA (European Union Agency for Cybersecurity) va procéder à la préparation d'un nouveau schéma de certification cybersécurité de la 5G. Cette étape fait suite à la boîte à outils développée par l'Union Européenne concernant la sécurité des réseaux 5G (Toolbox 5G). Elle devrait permettre d'améliorer la cybersécurité de ce type de réseaux, car elle contribue à éliminer certains risques.
A cet effet, ce schéma de certification cybersécurité sur la 5G sera fondé sur des dispositions déjà disponibles et sur des systèmes de certification cybersécurité existants ainsi que sur l'expérience déjà acquise par ENISA depuis qu'elle a commencé à s'engager dans la certification sur la cybersécurité. Ce programme est en cours et un appel à la recherche d'experts a été lancé au début de l'été 2021. Dès que ce schéma de certification sera existant pour la 5G, l'OFCOM va étudier les possibilités de l'utiliser.
Cependant, il existe déjà d'autres normes reconnues dans ce domaine, comme celles prescrites par GSMA NESAS (*Network Equipment Security Assurance Scheme*[35]*)*. GSMA NESAS est une initiative volontaire de l'industrie de la téléphonie mobile visant à lancer un programme d'amélioration continue de la sécurité pour les équipements et infrastructures des réseaux mobiles. GSMA NESAS couvre les équipements qui prennent en charge les fonctions définies par 3GPP et déployées par les opérateurs mobiles dans leurs réseaux. GSMA NESAS élabore des normes de sécurité et des certifications qui sont reconnues à large échelle au niveau mondial et auxquelles participe l'ensemble du secteur des télécommunications. Ce dernier a une grande confiance dans ces spécifications GSMA NESAS, ce qui garantit de ne pas ralentir les progrès techniques. A noter que GSMA NESAS ne couvre pas le déploiement des équipements de réseau, ni la configuration et l'exploitation des équipements de réseaux mobiles.
La GSMA a développé les exigences et les processus de sécurité pour NESAS en collaboration avec 3GPP, les opérateurs et les vendeurs d'équipements. La GSMA tient à jour une liste des fournisseurs d'équipements qui participent au programme et qui ont fait l'objet d'une évaluation de la sécurité de leurs processus de développement et de cycle de vie, ainsi que d'une évaluation de la sécurité de leurs produits réseau.
Dans sa version actuelle, GSMA NESAS comprend les éléments nécessaires à l'élaboration d'un système de certification. Dans le cadre de la conception d'un système de certification, GSMA NESAS définit:

- La nomination d'une organisation d'audit ;
- L'accréditation des laboratoires de test ;
- Les exigences de sécurité liées aux processus du fournisseur et aux produits de réseau, et les méthodes d'évaluation des processus des fournisseurs et des produits.

Certains fournisseurs d'équipements de réseaux mobiles (notamment chinois) ont fait l'objet d'une évaluation et d'un audit indépendant (laboratoires de tests certifiés par GSMA NESAS) de leurs processus de développement et de cycle de vie de certains produits. Ceci afin de démontrer comment la sécurité était intégrée dans leurs processus de conception, de développement, de mise en œuvre et de maintenance (par exemple pour les lignes de produits 5G gNodeB qui sont des stations de base).
Malgré les travaux réalisés jusqu'à présent, on ne sait toujours pas quelles normes et quel schéma de certification seront appliqués dans les pays européens. L'OFCOM précisera ces points dès que la réglementation

35 https://www.gsma.com/security/network-equipment-security-assurance-scheme/.

européenne sur la certification des installations de télécommunication critiques pour la sécurité aura été définie. Il est judicieux d'harmoniser les prescriptions suisses avec celles des pays de l'UE et d'éviter une solution purement suisse. En effet, le poids du marché européen devrait être exploité comme un avantage, car les produits utilisés en Suisse sont très probablement développés, fabriqués et testés ou certifiés à l'étranger.
L'al. 2 de la présente disposition prévoit que les concessionnaires de radiocommunication mobile exploitent leurs centres des opérations du réseau (Network Operations Centres) et leurs centres de gestion de la sécurité (Security Operations Centres) exclusivement dans des Etats dont la législation garantit une protection adéquate des données. L'art. 6, al. 1, de la loi fédérale sur la protection des données (LPD, RS 235.1) établit qu'aucune donnée personnelle ne peut être transmise à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée, notamment du fait de l'absence d'une législation garantissant une protection adéquate. Conformément à l'art. 7 de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD, RS 235.11), le Préposé fédéral à la protection des données et à la transparence publie une liste des Etats dont la législation garantit une protection adéquate des données. Dans la LPD totalement révisée (entrée en vigueur le 1er septembre 2023), la communication de données personnelles à l'étranger est régie par les art. 16 ss. L'évaluation du caractère adéquat des législations étrangères en matière de protection des données incombe au Conseil fédéral. En vertu de l'art. 8, al. 1, de la nouvelle ordonnance sur la protection des données (OPD), il publie la liste correspondante dans l'annexe 1. La limitation aux Etats figurant sur cette liste vise notamment à garantir que la communication transfrontalière de données par radiocommunication mobile satisfait aux exigences de la loi suisse sur la protection des données.
En vertu de l'art. II de l'annexe 1B à l'Accord instituant l'Organisation mondiale du commerce (Accord général sur le commerce des services, GATS, RS 0.632.20), les services et les fournisseurs de services de chaque membre de l'OMC doivent être traités de manière aussi favorable (clause de la nation la plus favorisée). A l'art. XIV, le GATS prévoit toutefois des exceptions, qui peuvent justifier des mesures si certaines conditions sont remplies. En particulier, l'art. XIV, al. c), autorise les mesures qui sont nécessaires pour garantir le respect des lois et réglementations. La limitation à des Etats disposant d'une protection adéquate des données, conformément à la législation sur la protection des données, est donc une mesure compatible avec les obligations de la Suisse dans le cadre de l'OMC.

Art. 96g Prescriptions applicables et surveillance

Pour assurer la sécurité des réseaux de téléphonie mobile à partir de la cinquième génération, l'OFCOM peut édicter des prescriptions techniques et administratives et déclarer obligatoires des normes techniques généralement reconnues sous forme de renvois statiques et directs (art. 96g, al. 1). Les projets de telles prescriptions et normes seront notifiés à l'Organisation Mondiale du Commerce (OMC) et à l'Association Européenne de Libre-Echange (AELE) en vertu des accords sur les entraves techniques au commerce conformément aux dispositions de l'Ordonnance du 17 juin 1996 (ON; RS 946.511) sur la notification des prescriptions et normes techniques ainsi que sur les tâches de l'Association suisse de normalisation. La preuve de la conformité aux normes peut être apportée par les fournisseurs concernés par exemple au moyen d'une certification par un organisme compétent dans le cadre du système suisse de l'accréditation (voir ordonnance du 17 juin 1996 sur l'accréditation et la désignation; RS 946.512) ou dans le cadre d'autres systèmes de certification (GSMA NESAS, schémas européens de certification de cybersécurité[36]). A défaut d'une certification sur une base volontaire de leur système de gestion de la sécurité (art. 96e) ou s'il n'est pas certain que les installations de télécommunication critiques pour la sécurité correspondent à l'état de la technique (art. 96f, al. 1), un concessionnaire de radiocommunication mobile pourra, dans le cadre de la surveillance, être obligé, à ses frais, de se soumettre à un audit ou de faire tester ses installations de télécommunication auprès d'un organisme disposant des qualifications nécessaires, et de remettre à l'OFCOM les résultats de cet audit ou de ce test (al. 2). Une telle mesure ne pourra toutefois être prise que dans le cadre de l'art. 58, al. 2, LTC, s'il existe un soupçon fondé que le concessionnaire ne respecte pas les exigences découlant des art. 96e et 96f et que l'OFCOM n'est pas en mesure de constater lui-même les faits pertinents. Elle serait en revanche exclue en l'absence d'un tel soupçon, notamment dans le cadre de la surveillance générale au sens de l'art. 58, al. 1, LTC (campagnes de surveillance). Il s'agira en outre de veiller à ce que l'organisme qualifié

36 Voir règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité), JO L 151/15.

traite de manière confidentielle les informations auxquelles il aura accès, en particulier celles en lien avec une éventuelle mesure de surveillance au sens de la LSCPT.

4 Conséquences

4.1 Conséquences pour la Confédération

4.1.1 Sécurité des réseaux de radiocommunication mobile à partir de la 5e génération

Les conséquences pour la Confédération en termes de finances, de personnel et autres ont été examinées Dans un premier temps, elles seront probablement insignifiantes. La mise en œuvre et la prise en charge des coûts devront initialement être assurées par les entreprises. L'OFCOM devra toutefois assumer des dépenses supplémentaires, difficilement quantifiables à l'heure actuelle, dans le domaine de la normalisation et de la surveillance en lien avec la sécurité des réseaux mobiles 5G et les futures technologies. Par ailleurs, les tâches supplémentaires dans le domaine de la normalisation et de la surveillance devront être intégrées dans les processus de travail existants de l'OFCOM. Il conviendra toutefois de suivre de près l'évolution de la situation à cet égard.

4.1.2 Manipulation non autorisée d'installations de télécommunication

Les conséquences pour la Confédération en termes de finances, de personnel et autres ont été examinées; dans l’ensemble, elles seront probablement insignifiantes. Le NCSC informe déjà les fournisseurs sur de possibles cyberattaques dans ou depuis leur réseau, un élément qui revêt une grande importance pour la cybersécurité de la Suisse. La tâche du NCSC décrite dans l'ordonnance peut donc être réalisée avec les ressources existantes. A l'OFCOM, les nouvelles tâches dans le domaine de la cybersécurité et leur exécution conjointe avec le NCSC requièrent un à deux postes supplémentaires. Le NCSC dispose d'un pool de travail à cette fin. Par le passé, l'OFCOM avait déjà exprimé un besoin, mais celui-ci n'avait pas été pris en compte. Au vu des présentes dispositions, il est désormais suffisamment concret. Dans l'ensemble, il n'y a pas de conséquences pour la Confédération, car le pool de travail existe déjà.

4.2 Conséquences économiques

4.2.1 Sécurité des réseaux de radiocommunication mobile à partir de la 5e génération

Les quatre mesures proposées pour la sécurité de la 5G impliquent des coûts pour les trois concessionnaires de radiocommunication mobile actifs en Suisse.
Entre fin mars et mi-mai 2021, l'OFCOM a mené auprès de ceux-ci une enquête sur les mesures techniques de la Toolbox 5G qu'ils ont prises ou prévues, ainsi que sur leurs coûts.
Les résultats ont montré que les fournisseurs attachent une grande importance à la norme ISO 27001 pour leurs systèmes de gestion de la sécurité de l'information (SGSI). Les exigences spécifiées dans les prescriptions techniques et administratives doivent également se référer à ces normes et à des normes comparables. Pour les concessionnaires, il ne faut donc pas s'attendre à des changements ni à des coûts majeurs par rapport à la situation actuelle.
Les résultats ont également montré que les concessionnaires de radiocommunication soutiennent la certification des éléments de réseau et demandent que leurs fournisseurs soient aussi soumis à certaines exigences de sécurité. Ils donnent la priorité aux normes internationales, en premier lieu au GSMA NESAS. La réglementation dans ce domaine n'entraînerait vraisemblablement pas de coûts supplémentaires importants. L’obligation qui leur est imposée d’avoir leurs centres des opérations du réseau et de gestion de la sécurité exclusivement dans les Etats dont la législation garantit une protection adéquate des données est déjà remplie.
Les concessionnaires de radiocommunication mobile ont décrit de manière plus ou moins détaillée les mesures qu'ils ont prises. Souvent, ils ont fourni peu d'informations, ou n'en ont pas fourni du tout, sur les coûts spécifiques associés aux mesures. Par conséquent, seules des considérations qualitatives sur les coûts peuvent être données.
Les concessionnaires de radiocommunication mobile sont aussi susceptibles d'encourir des coûts liés à d'éventuelles obligations de se soumettre à un audit. Toutefois, en particulier si le niveau de conformité aux

normes pertinentes est élevé, les audits devraient être peu fréquents; en effet, le concessionnaire ne peut être obligé de procéder à ses frais à un audit que dans le cadre de l'art. 58, al. 2, LTC, lorsqu'il est présumé de manière fondée que le concessionnaire ne respecte pas les exigences des art. 96e et 96f et que l'OFCOM n'est pas en mesure d'établir lui-même les faits. Les coûts d'un audit individuel dépendent de l'étendue de l'examen. Selon les estimations, dans la plupart des cas, il devrait s'agir d'un montant à cinq chiffres[37].

Le bénéfice pour l'économie résulte de l'évitement des coûts que les ménages, les entreprises et les autres groupes sociaux pourraient encourir en cas de risques liés à la sécurité des réseaux mobiles. Par exemple, les pannes dans la couverture des communications mobiles ont des conséquences potentiellement graves. La radiocommunication mobile[38] joue un rôle de plus en plus important auprès des internautes[39] et des entreprises[40]. Dans son dossier sur les dangers "Panne d'un réseau de téléphonie mobile", l'OFPP calcule qu'une panne totale de trois jours chez un grand opérateur mobile entraînerait des pertes globales de l'ordre de neuf milliards de francs suisses. Toutefois, une telle panne - très improbable[41], mais à ne pas négliger vu l'ampleur des dommages mentionnés - n'est qu'une conséquence possible. Des lacunes sécuritaires dans l'exploitation et l'infrastructure des réseaux mobiles peuvent ouvrir la voie à toutes sortes de cyberattaques sur les données et les applications basées sur la 5G (ou les technologies suivantes), comme le vol de données et le chantage. Une étude relativement récente sur les petites et moyennes entreprises (PME) montre qu'un quart des PME suisses interrogées ont déjà été victimes d'une cyberattaque, dont un tiers ont subi un préjudice financier et, dans une moindre mesure, une perte de données clients et/ou une atteinte à leur réputation[42]. Une étude autrichienne montre que, même dans une période de pandémie économiquement difficile, près des trois quarts des entreprises interrogées ont augmenté leur budget pour la cybersécurité[43]. Comme décrit, cependant, ces conséquences potentielles bénéfiques pour l'économie sont indirectes. En outre, la probabilité d'une panne, par exemple, peut difficilement être imputée à des mesures de sécurité spécifiques. Les dommages potentiels des cyberrisques sont également difficiles à évaluer[44]. Par conséquent, le bénéfice des mesures proposées ne peut être quantifié.

4.2.2 Manipulation non autorisée d'installations de télécommunication

Le bénéfice pour l'économie résulte de l'évitement des coûts que peuvent engendrer les cyberattaques pour les ménages, les entreprises et les autres groupes sociaux. Les coûts économiques des cyberattaques décrits aux chiffres **Fehler! Verweisquelle konnte nicht gefunden werden.** et 1.2.3 et aux deux premiers points à examiner dans l'analyse d'impact de la réglementation (AIR) sont élevés et ont fortement augmenté ces dernières années. Ils sont toutefois difficiles à calculer. D'une part, les victimes d'une cyberattaque ne la rendent pas toujours publique et d'autre part, il est très difficile de mesurer correctement les coûts indirects des cyberattaques (p. ex. l'atteinte à la réputation, la perte de confiance, le mécontentement des clients). En outre, les bénéficies peuvent difficilement être imputés à des mesures de sécurité particulières. Cependant, il est incontestable que les dommages causés par les cyberattaques pèsent depuis longtemps, et de manière importante, sur l'économie. Les mesures visant à réduire ces coûts ont donc un effet positif direct.

37 Cette estimation se base sur les valeurs de référence fournies par la plateforme d'offres gryps.ch pour les PME comptant 60 employés (GRYPS]2021]: *ISO Zertifizierung Kosten*, https://www.gryps.ch/produkte/iso-9001-zertifizierung-178/kosten/). Pour un audit de certification initial, par exemple, on l'estime à titre indicatif à 16'000 francs. D'un côté, les opérateurs de réseaux mobiles sont beaucoup plus grands, ce qui signifie qu'il faut s'attendre à des coûts beaucoup plus élevés pour un audit. D'autre part, le champ à auditer est généralement beaucoup plus restreint que dans le cas d'un audit de certification initiale, ce qui réduit les coûts. En raison de ces effets contraires, il semble probable que les coûts résultants seront inférieurs à 100'000 francs.

38 Comme décrit au chiffre 1.1.1, la radiocommunication mobile passe de plus en plus par la 5G.

39 Selon l'OFS (2020): *Utilisation mobile d'internet,* https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/haushalte-bevoelkerung/mobile-internetnutzung.assetdetail.12307308.html, 84% des internautes suisses âgés de 16 à 74 ans ont utilisé un téléphone mobile en 2019.

40 Selon l'OFS (2019): *Infrastructure TIC dans les entreprises,* https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/unternehmen/ikt-infrastruktur.assetdetail.8486582.html, 77 % des entreprises ont utilisé des connexions mobiles à large bande en 2017.

41 La probabilité d'une telle panne (Scénario 2 - élevée) est de une fois tous les 30 ans. OFPP (2020): *Panne d'un réseau de téléphonie mobile*, https://www.babs.admin.ch/de/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse/gefaehrddossier.html. La base méthodologique est décrite dans OFPP (2020): *Méthode d'analyse nationale des risques*, https://www.babs.admin.ch/de/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse.html.

42 Peter et al. (2020): *Digitalisierung, Home-Office und Cyber-Sicherheit in KMU,* https://www.fhnw.ch/de/die-fhnw/hochschulen/hsw/media-newsroom/news/digitalisierung-home-office-und-cyber-sicherheit/media/digitalisierung-home-office-cyber-sicherheit-kmu-2020-12.pdf ansi que Rapport final de Gfs Zurich (2020) : *Vague de télétravail dans les PME suisses: Les opportunités saisies s'accompagnent d'une sous-estimation des cyberrisques,* https://gfs-zh.ch/homeoffice-welle-in-schweizer-kmuchancen-wahrgenommen-cyberrisiken-unterschaetzt/.

43 KPMG (2021): *KPMG Studie: Cyberrisiken werden durch die Pandemie beschleunigt,* https://home.kpmg/at/de/home/media/press-releases/2021/04/kpmg-studie-cyberrisiken-werden-durch-die-pandemie-beschleunigt.html.

44 Biener et al. (2015): *Cyber Risk: Risikomanagement und Versicherbarkeit*, https://www.kessler.ch/fileadmin/09_PDFs/Cyber_Risk_Risikomanagement_und_Versicherbarkeit_de.pdf.

Il est généralement admis que la cybersécurité deviendra de plus en plus un facteur de compétitivité pour la numérisation[45]. Pour que la Suisse puisse aussi utiliser ses avantages dans l'économie numérique, elle doit créer les conditions nécessaires au niveau réglementaire. Les exigences minimales de sécurité imposées aux fournisseurs d'accès à Internet contribuent à permettre l'exploitation du potentiel économique de la numérisation.
Alors que les mesures proposées auront un effet positif tant du point de vue macroéconomique que social (voir chiffre 4.3.2), elles engendrent aussi des coûts pour les fournisseurs d'accès Internet. Or, ces coûts ne sont pas quantifiables, car de nombreux facteurs, tels que l'ampleur des mesures déjà mises en œuvre aujourd'hui par les fournisseurs ou la réduction des coûts grâce aux développements techniques, sont très difficiles à déterminer. Il s'agit donc ci-après d'une évaluation qualitative des coûts et d'un examen des conséquences auxquelles s'attendre, notamment pour les petits fournisseurs. En 2019, cinq grands FAI détenaient 86% des parts de marché en termes de clientèle. Dans le même temps, ces entreprises ne représentent qu'une fraction de tous les FAI opérant en Suisse. Au total, près de 170 fournisseurs d'accès Internet sont actifs en Suisse: 60% ont entre 1 et 1'000 clients, 25% entre 1'000 et 10'000 clients et 15% en ont plus de 10'000[46].

4.2.2.1 Coûts de la mesure 1: Droit de bloquer ou de restreindre les accès à Internet et les ressources d'adressage, et obligation d'informer les clients

Puisque le blocage ou la restriction du raccordement Internet relèvent de l'appréciation des fournisseurs, ces mesures ne génèrent des coûts que si les fournisseurs décident de les appliquer. Dans ce cas également, les coûts sont faibles et servent l'intérêt des fournisseurs. En ce qui concerne l'obligation d'informer, les fournisseurs supportent au moins les mêmes coûts que s'ils n'informent pas activement les clients du blocage ou de la restriction de leurs raccordements, car on peut supposer que ceux-ci les contacteront très probablement de leur propre chef. Dans un cas comme dans l'autre, le service clients engendre des coûts.

4.2.2.2 Coûts de la mesure 2: Obligation pour les fournisseurs de filtrer les paquets IP dont l'adresse IP source est falsifiée (spoofing)

L'introduction de méthodes de filtrage des paquets IP dont l'adresse IP source est falsifiée exige des fournisseurs un effort technique et administratif. Ils doivent implémenter les filtres et identifier les réseaux autorisés. Ils doivent également mettre à jour les filtres en permanence afin qu'aucun paquet IP légitime ne soit filtré. Cependant, comme la méthode du filtrage à l'entrée a été développée il y a 20 ans, sa mise en œuvre est devenue beaucoup plus facile. Il existe de nombreux outils et lignes directrices librement accessibles et les obstacles techniques à la mise en place ont fortement diminué ces dernières années[47].
Pour l'évaluation des coûts, il est important de noter que ceux des petits fournisseurs sont nettement inférieurs à ceux des grands prestataires[48]. Les petits fournisseurs ont beaucoup moins d'efforts à fournir pour déterminer quels réseaux sont autorisés et sont également confrontés à des exigences moins complexes lors de l'exploitation du filtre. En outre, les connexions sortantes contenant des éléments d'adressage falsifiés ne doivent être empêchées que si cela est techniquement possible pour les fournisseurs d'accès Internet avec des moyens raisonnables.

4.2.2.3 Coûts de la mesure 3: Obligation pour les fournisseurs de configurer de manière sûre les terminaux mis à la disposition des clients

La mesure 3 peut entraîner une hausse des prix pour les fournisseurs en ce qui concerne l'acquisition et la maintenance des terminaux. Les accords contractuels avec les fabricants de terminaux sont déterminants.

45 Bundesamt für Sicherheit in der Informationstechnik (2016): *Cyber-Sicherheit als Wettbewerbsvorteil in der Digitalisierung,* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Cyber-Sicherheit_als_Wettbewerbsvorteil.pdf?__blob=publicationFile&v=3.

46 OFCOM (2021 sur la base des chiffres de la statistique des télécommunications de 2019). Voir aussi *Les Internet Service Providers,* https://www.bakom.admin.ch/bakom/de/home/telekommunikation/zahlen-und-fakten/sammlung-statistischer-daten/internet-service-provider.html.

47 MANRS (2016-2021): *Anti-Spoofing,* https://www.manrs.org/isps/guide/antispoofing/.

48 Lone et al. (2020): *SAVing the Internet: Explaining the Adoption of Source Address Validation by Internet Service Providers*, https://weis2020.econinfosec.org/wp-content/uploads/sites/8/2020/06/weis20-final31.pdf.

Les exigences techniques applicables aux appareils peuvent être respectées à moindres coûts par les fabricants. Toutefois, les fournisseurs doivent s'assurer qu'ils sont contractuellement tenus de le faire. Ils sont également responsables des mesures de sécurité pour la maintenance à distance, de l'installation rapide des mises à jour de sécurité et du remplacement des terminaux à la fin de leur durée de vie. Cependant, l'effort requis est généralement faible car les fabricants livrent les mises à jour nécessaires. Le risque et les dépenses de maintenance d'un terminal non sécurisé ou obsolète peuvent être plus coûteux à long terme qu'une configuration et une maintenance appropriées.
La mesure 3 aura également tendance à entraîner des coûts plus élevés pour les grands fournisseurs que pour les petits fournisseurs. Ces derniers ont moins de terminaux en service et peuvent donc assurer une configuration et une maintenance sécurisées avec moins de ressources.
A relever que la réglementation à l'art. 96a, al. 3, ne concerne que les équipements et appareils mis à disposition des clients par les FAI. Si le client acquiert son appareil auprès d'un fournisseur tiers, il ne supporte aucun coût. Après la livraison de l'appareil, des coûts supplémentaires, par exemple pour l'installation de mises à jour de sécurité, ne sont dus que si le FAI détient toujours le contrôle de l'appareil.

4.2.2.4 Coûts de la mesure 4: Obligation pour les fournisseurs d’exploiter un service spécialisé dans le signalement de manipulations, et de prendre des mesures de défense

L'obligation de désigner un service qui assure dans les délais impartis une réponse aux signalements entraîne des coûts pour les fournisseurs n’ayant pas encore mis en place ce type de service. Toutefois, le temps de réaction dans un délai raisonnable évite aux fournisseurs d'avoir à maintenir un service de piquet pendant la nuit ou le week-end. En outre, les fournisseurs peuvent consulter le NCSC pour savoir si le signalement par le NCSC peut également se faire par d'autres canaux, ce qui leur permet de garantir une capacité de réaction dans un délai raisonnable et au moindre coût possible. Les coûts pour les FAI sont compensés par un avantage important en matière de protection, car seule une réaction rapide peut réduire le risque de compromettre les autres raccordements. Les coûts liés à la réaction et aux mesures de lutte sont difficiles à quantifier car ils varient fortement en fonction du fournisseur et, surtout, de la menace. Par ailleurs, les menaces et les mesures appropriées des FAI évoluent elles aussi constamment.

4.3 Conséquences pour la société

4.3.1 Sécurité des réseaux de radiocommunication mobile à partir de la 5e génération

Les conséquences pour la société, en particulier pour la santé et la sécurité, peuvent aussi être vues comme bénéfiques. Par exemple, le dossier de l'OFPP sur les dangers mentionnés au point 4.2 (Conséquences pour l'économie) considère également qu'une panne de la radiocommunication mobile peut avoir des conséquences multiples et entraîner des décès, des blessures et des restrictions des activités des services d'urgence.

4.3.2 Manipulation non autorisée d'installations de télécommunication

La numérisation a des conséquences majeures pour la société car elle touche directement la vie quotidienne des gens. Les cyberincidents provoquent parmi la population un sentiment d'insécurité lors de l'utilisation des offres numériques. Il est important pour la confiance générale dans les technologies numériques que celles-ci répondent à un niveau minimal de sécurité. Lorsque les consommateurs acquièrent un appareil auprès d'un FAI, ils devraient pouvoir partir du principe que celui-ci est configuré, comme le requiert la mesure 3, de manière à ce qu'il soit protégé de manière minimale contre les cyberattaques.

4.4 Conséquences dans d'autres domaines

4.4.1 Sécurité des réseaux de radiocommunication mobile à partir de la 5e génération

Les conséquences possibles pour les cantons et les communes ainsi que pour les centres urbains, les agglomérations et les régions de montagne ou pour l'environnement ont été examinées. Les réseaux 5G et les réseaux sécurisés des générations suivantes peuvent avoir des conséquences bénéfiques indirectes. Cependant, celles-ci ne sont pas spécifiques et ne concernent pas seulement les applications et les utilisateurs

de la 5G. Par conséquent, les conséquences ne sont pas examinées en détail. Les avantages généraux attendus sont décrits aux points 4.2 (Conséquences pour l'économie) et 4.3 (Conséquences pour la société).

4.4.2 Manipulation non autorisée d'installations de télécommunication

Les conséquences possibles pour les cantons et les communes ainsi que pour les centres urbains, les agglomérations et les régions de montagne ou pour l'environnement ont été examinées. Un niveau de sécurité plus élevé peut avoir des conséquences bénéfiques indirectes. Cependant, celles-ci ne sont pas spécifiques et ne sont donc pas examinées en détail. Les avantages généraux attendus sont décrits aux points 4.2 (Conséquences pour l'économie) et 4.3 (Conséquences pour la société).

5 Aspects juridiques

Les dispositions proposées mettent en œuvre l'art. 48*a* LTC. L'al. 2 de cette disposition délègue au Conseil fédéral de larges compétences législatives dans le domaine de la sécurité des informations et des infrastructures et services de télécommunication. Selon l'art. 62, al. 2, LTC, le Conseil fédéral peut déléguer à l'OFCOM le soin d'édicter les prescriptions techniques et administratives nécessaires (voir aussi l'art. 105, al. 1, OST). Ce faisant, l'OFCOM devra tenir compte des normes applicables au niveau international. L'Union européenne met en particulier en place un schéma de certification de cybersécurité dans le domaine des réseaux 5G (voir commentaire art. 96*g*), dont il conviendra de s'inspirer dans la mesure du possible s'agissant des art. 96*d* à 96*g*.
L'obligation de localisation des centres des opérations du réseau et de gestion de la sécurité dans des pays spécifiques prévue à l'art. 96*f*, al. 2, est compatible avec l'art. XIV, let. c, ii et iii de l'annexe 1B à l'Accord instituant l'Organisation mondiale du commerce (Accord général sur le commerce des services, GATS) (voir commentaires art. 96*f*, al. 2).

Liste des abréviations

AIR	Analyse d'impact de la réglementation
API	*Application Programming Interface*
ASA	Association suisse d'assurances
BCP	*Best Current Practices*
CENAL	Centrale nationale d'alarme
CPE	*Customer Premises Equipment* - Equipement terminal
DDoS	*Distributed Denial Of Service attack*
ENISA	*European Union Agency for Cybersecurity*
ETIS	*The Community for Telecom Professionals*
FDI	*Foreign* Direct Investment
FST	Fournisseur d'accès à Internet
IETF	*Internet* Engineering Task Force
IP	*Internet Protocol* – Protocole internet
ISO	*International Organization for Standardization* – Organisation internationale de normalisation
LPD	Loi fédérale sur la protection des données (RS 235.1)
LTC	Loi sur les télécommunications
M3AAWG	*Messaging Malware Mobile Anti-Abuse Working Group*
MANRS	*Mutually Agreed Norms for Routing Security*
MNO	*Mobile Network Operator*
NCSC	Centre national pour la cybersécurité
NOC	*Network Operation Center* – Centre d'opérations des réseaux
OFCOM	Office fédéral de la communication
OFPP	Office fédéral de la protection de la population
PMU	Petites et moyennes entreprises
RIR	*Regional Internet Registry* - Registre Internet régional
SANS	*SysAdmin, Audit, Network, Security Institut*
SGSI	Système de gestion de la sécurité de l'information
SOC	*Security Operation Center* - Centre de gestion de la sécurité
UIT	Union internationale des télécommunications