Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Berne, le 16 novembre 2022

Révision de l'Ordonnance sur les services de télécommunications (OST)

Rapport rendant compte des résultats de la procédure de consultation (3 décembre 2021 au 18 mars 2022)

Table des matières

1 Introduction

L'art. 48*a* de la loi sur les télécommunications donne au Conseil fédéral la compétence de réglementer la sécurité des informations et des infrastructures et services de télécommunication. Le 3 décembre 2021, il a lancé une consultation concernant une modification de l'ordonnance sur les services de télécommunication (OST) afin de mettre en œuvre cette compétence. Les adaptations proposées concernent l'annonce des perturbations, la lutte contre les manipulations non autorisées des installations de télécommunication ainsi que la sécurité des réseaux de téléphonie mobile de dernière génération (5G). Les cantons, les partis politiques représentés à l'Assemblée fédérale ainsi que les milieux intéressés étaient invités à donner leur avis jusqu'au 18 mars 2022. Le projet mis en consultation a fait l'objet de 46 avis. La liste des participants et des abréviations par lesquelles ils sont désignés figure en annexe. Les avis peuvent être consultées sur le site Internet de l'OFCOM (www.ofcom.admin.ch > L'OFCOM > Organisation > Bases légales > Consultations 2021).

L'avis de la **CG-MPS** a été repris tout ou partie ou avec des variations par les cantons **BL**, **JU**, **AI**, **AR**, **LU**, **TG**, **NW**, **FR**, **BE**, **TI**, **GR**, **AG**, **OW**, **GE**, **GL**, ainsi que par IVR, la **CCPCS**, **KAPO AI**, **Gebäudeversicherung Kanton Zug**, la **CCDJP** et **FKS.**

SUISSEDIGITAL renvoie à l'avis de son membre **Sunrise UPC** concernant les mesures spécifiques qui s'appliquent aux réseaux de radiocommunication mobile de 5e génération.

2 Remarques générales

La **COMCO** et les cantons **Uri**, **SH**, **BS, VS** ainsi que **SBV** et le **PS** approuvent ou soutiennent sans autres commentaires ou propositions de modifications le projet d'ordonnance mis en consultation.

La **CG-MPS**, les cantons **JU**, **BL**, **TG**, **AI**, **AR**, **SO**, **SG**, **LU**, **NW**, **FR**, **BE**, **TI**, **ZG**, **GR**, **OW**, **GE**, **GL**, **VD**, **NE**, ainsi que **Internetverband für Rettungswesen**, **la CCPCS**, **KAPO AI**, **Gebäudeversicherung Zug**, **Staatskanzlei ZH**, la **CCDJP**, l'**asut**, **Sunrise UPC**, **Swisscom**, la **SSR**, **digitalswitzerland**, **Salt**, la **FER**, **FKS**, **economiesuisse** sont d'accord avec le projet d'ordonnance de manière générale, mais ont formulé des commentaires ou des propositions de modification.

L'**UDC Suisse** salue certes l'établissement d'exigences minimales dans le domaine de la sécurité des infrastructures de télécommunication, mais ne peut pas approuver le projet d'ordonnance sous cette forme.

Le thème de la sécurité des informations et des infrastructures de télécommunication constitue pour **SUISSEDIGITAL** un thème stratégique central. L'association estime que les mesures proposées en matière d'exploitation des infrastructures et des services de télécommunication sont inévitablement liées à une augmentation des investissements et des coûts d'exploitation pour ses membres, ce qui, en fin de compte, concerne également les clients de ses membres.

L'**USP** estime que les nouvelles réglementations de l'OST contribuent à soutenir le développement numérique puisqu'elles établissent de manière obligatoire des normes et des mesures de sécurité minimales et favorisent ainsi la confiance des utilisateurs et des entreprises dans la numérisation et les applications qui y sont liées.

Le **Centre Patronal** approuve les adaptations proposées, mais laisse toutefois le soin aux fournisseurs de services concernés de se prononcer sur le caractère praticable ou suffisant des efforts demandés.

L'**asut** salue la révision proposée de l'OST. Selon elle, cette révision a du potentiel pour renforcer encore la confiance de l'économie et de la société envers la sécurité des réseaux de télécommunication en tant qu'infrastructure critique.

Selon **Sunrise UPC,** une modification des bases légales ne serait pas indispensable. Grâce à différents instruments établis, l'entreprise assure déjà aujourd'hui les standards de sécurité les plus élevés et met ainsi déjà en œuvre la plupart des mesures proposées.

Swisscom partage l'avis du Conseil fédéral selon lequel il convient d'accorder une attention particulière à la sécurité des réseaux et des services de télécommunication, et de prendre les mesures nécessaires. Il lui semble important que des délais de mise en œuvre suffisants soient prévus.

La **SSR** estime en outre important que le deuxième paquet de mesures, destiné à garantir l'approvisionnement en électricité, soit adopté.

3 Remarques sur les dispositions de l'avant-projet

Art. 96 Signalement de perturbations

IVR, la **CCPCS**, la **CCDJP,** la **CSSP, GVZG**, la **CG-MPS**, les cantons **AG**, **AI**, **AR**, **BE, BL**, **FR**, **GE**, **GL**, **LU**, **NW**, **OW**, **SO**, **TG**, **TI**, **VD**, **ZG** et **Kapo AI** suggèrent que les processus d'alarme et d'annonce ou les rôles des différents acteurs et services soient décrits en détail.

Al. 1

La **CG-MPS**, **IVR**, la **CCPCS**, la **CCDJP**, la **CSSP**, **Kapo AI**, **GVZG**, les cantons **BL**, **AI**, **AR**, **TG**, **SO**, **SG**, **LU**, **FR**, **NW**, **BE**, **TI**, **AG**, **OW**, **GL**, **GR**, **ZG** et **GE** demandent que les valeurs seuils d'une perturbation à signaler soient abaissées à 1’000 clients concernés pendant au moins 15 minutes, et 10 minutes pour le **canton du JU**.

Swisscom veut s'en tenir aux seuils actuels de 30’000 clients concernés et d'une heure.

IVR, la **CCPCS**, la **CCDJP**, la **CSSP,** l'**UDC**, **GVZG**, **Economiesuisse**, **Swisscom**, les cantons **SO**, **SG**, **BE**, **OW** et **Kapo AI** demandent que la valeur seuil des clients concernés continue à être réglée dans les prescriptions techniques et administratives (PTA) et non au niveau de l'OST. Selon eux, cela permet une adaptation rapide aux nouvelles circonstances.

Swisscom et **Salt** approuvent la CENAL en tant que centrale de signalement.

IVR, la **CCPCS**, la **CCDJP**, la **CSSP, GVZG**, **Kapo AI**, les cantons **SO**, **SG**, **BE**, **OW** et **VD** insistent sur le fait que les fournisseurs de services de télécommunication doivent informer les centrales d'appel d'urgence cantonales compétentes avant que les messages ne soient envoyés à la CENAL ou à d'autres organes.

L'**asut**, **Sunrise UPC**, **Digital Switzerland** et **Economiesuisse** soulignent que les compétences des différentes autorités auxquelles les fournisseurs de services de télécommunication doivent signaler les incidents doivent être clairement définies et leur nombre aussi limité que possible. Il est également proposé de désigner le NCSC (*National Cyber Security Centre*) plutôt que la CENAL comme centrale de signalement. Il est important de coordonner la révision de l'OST et la modification de la loi sur la sécurité de l'information (LSI).

Al. 2

IVR, la **CCPCS**, la **CCDJP,** la **CSSP**, **SO** ainsi que les cantons **FR**, **TI**, **OW**, **GE**, **GL** et **VD** désapprouvent le fait que l'OST règle exclusivement la transmission à l’OFCOM de l'information relative aux perturbations signalées par la CENAL. Ils estiment que le NCSC, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) ainsi que les centrales d'alarme cantonales de la police, des pompiers et des services sanitaires devraient également être impliqués. **Swisscom** et **Economiesuisse** soutiennent la transmission de l'information à d'autres autorités.

Salt demande que les données relatives aux annonces de perturbation ne soient pas publiées car elles pourraient donner lieu à des comptes-rendus erronés dans les médias. Les perturbations signalées ne doivent être publiées que sous forme agrégée.

Art. 96a Manipulation non autorisée d'installations de télécommunication (mesures de sécurité)

Al. 1

IVR, la **CCPCS**, la **CCDJP**, les cantons **BE**, **SG**, **OW**, **VD**, la **KAPO AI**, **GVZG** et la **CSSP** demandent que la réglementation ne soit pas limitée exclusivement aux attaques DDoS. Celles-ci devraient plutôt être mentionnées notamment à titre d'exemple. En outre, ils font valoir que les détails des mécanismes d'attaque potentiels ne doivent pas être réglés de manière exhaustive dans l'OST, mais dans les PTA. Cela permet d'agir de manière adéquate et d'adapter de manière simple les réglementations à prendre en compte.

Le canton **GE** affirme que les opérateurs devraient utiliser tous les moyens techniques raisonnables pour configurer leurs réseaux selon les meilleures pratiques de sécurité, y compris le contrôle des ressources d'adressage falsifiées.

Economiesuisse fait valoir qu'il faut prévoir des délais de mise en œuvre et des délais d'anticipation suffisants (au moins 6 mois) et les définir dans les PTA.

Al. 2

Economiesuisse, l'**UDC** et **Swisscom** souhaitent que le champ d'application soit clairement délimité. La mise à jour des smartphones doit être laissée à l'appréciation des utilisateurs finaux et ne doit pas tomber sous le coup de cette disposition. Selon **SUISSEDIGITAL**, il faut préciser que la disposition s'applique exclusivement aux appareils remis par des fournisseurs d'accès à Internet.

Economiesuisse et **Swisscom** plaident pour des délais de mise en œuvre suffisants (au moins 6 mois).

Selon **economiesuisse,** les équipements terminaux (Customer Premises Equipment) doivent être réglementés par une norme de sécurité de base. En outre, sur certains points, les exigences imposées par la réglementation doivent être davantage liées à la faisabilité technique.

Selon la **FER**, la résilience numérique ne peut être atteinte que par une prise en compte globale de toutes les différentes facettes des cyberrisques.

Salt demande une actualisation "régulière" plutôt que "sans délai".

Pour la **SSR,** les mesures de sécurité ne vont pas assez loin, car elles sont prévues pour les équipements terminaux, et l'obligation ne s'applique qu'aux fournisseurs d'accès Internet. L'objectif devrait être de protéger tous les terminaux exposés.

Swisscom souhaite laisser aux fournisseurs d'accès Internet le soin d'évaluer si les installations de télécommunication doivent être modernisées.

Divers avis s'expriment déjà sur la mise en œuvre technique concrète de la disposition. Certains se réfèrent explicitement aux principes relatifs aux PTA énoncés dans le rapport explicatif.

Selon l'**asut**, **digitalswitzerland** et **Sunrise UPC,** le principe relatif aux PTA concernant la fin de vie des équipements terminaux devrait être reformulé. Ce n'est que lorsque ceux-ci ne sont plus soumis à des mises à jour de sécurité jugées critiques qu'ils devraient être remplacés. **Swisscom** ne souhaite pas laisser aux seuls fabricants le soin d'évaluer si les installations doivent être remplacées pour des raisons de sécurité. Les fournisseurs d'accès Internet doivent être impliqués.

L'**asut** et **Sunrise UPC** souhaitent la suppression du principe selon lequel les services non utilisés doivent être désactivés sur les équipements terminaux. Selon **Swisscom**, certains ports de ces équipements devraient être ouverts à l'état de livraison pour pouvoir être configurés via le système de télémaintenance.

SUISSEDIGITAL et **Salt** souhaitent se baser sur des normes internationales.

Swisscom estime qu'il est nécessaire, dans le cadre du processus de support, de discuter préalablement avec les fournisseurs d'accès Internet au sujet des modifications spécifiques à la sécurité des accès au routeur limités dans le temps et dans leur contenu et d'examiner les alternatives possibles. De manière générale, les PTA doivent être soumises au préalable aux fournisseurs d'accès Internet concernés. En outre, elles ne doivent pas être restrictives au point de compliquer inutilement, voire de rendre impossible, la gestion des équipements terminaux par les fournisseurs d'accès Internet.

Al. 3

La **CSSP**, l'**Assurance immobilière de Zoug**, les cantons **BE**, **GE**, **OW**, **SO**, **SG**, **VD**, **Kapo AI**, la **CCDJP**, la **CCPCS** et **IVR** demandent que les blocages ou les restrictions d'utilisation des accès Internet ou des ressources d'adressage soient très sélectifs. Ce n'est que dans des cas exceptionnels qu'ils peuvent entraîner l'impossibilité de composer des numéros d'urgence via les raccordements concernés.

La **CSSP**, l'**Assurance immobilière de Zoug**, les cantons **BE**, **OW**, **SO**, **Kapo AI**, la **CCDJP**, la **CCPCS** et **IVR** demandent que les centrales d'appel d'urgence cantonales concernées soient informées si les restrictions risquent de toucher plus de 1'000 clients pendant plus de 15 minutes.

Les cantons **AG**, **AI**, **AR**, **BL**, **GL**, **LU**, **NW**, **TI**, **TG**, **ZG** et la **CG-MPS** demandent l'introduction d'une obligation de blocage des accès Internet ou des ressources d'adressage qui présentent un risque pour les infrastructures critiques.

Selon le canton **BL**, les fournisseurs d'accès Internet doivent être tenus d'aider les clients concernés par des coupures ou une utilisation limitée à résoudre le problème de sécurité sous-jacent. De manière générale, ils doivent rétablir l'accès à Internet le plus rapidement possible.

Le canton **TI** demande que les analyses de données effectuées par les fournisseurs d'accès Internet dans le cadre du blocage de l'accès à Internet ne portent pas atteinte à la protection des données.

Le canton **ZG** souhaite que, pour éviter les déchets électroniques, des réglementations complémentaires soient étudiées auprès des vendeurs et des fabricants d'équipements de télécommunication.

Swisscom est d'avis que des activités nuisibles pourraient également provenir de raccordements surveillés en vertu de la LSCPT. Afin de protéger les réseaux et les services, ceux-ci devraient également pouvoir être bloqués par les fournisseurs d'accès Internet, notamment en cas de risque important pour la sécurité et la stabilité des installations de communication. Pour la mise en œuvre des mesures de sécurité, tant sur le réseau fixe que sur le réseau mobile, il convient d'accorder des délais appropriés et d'associer étroitement les fournisseurs d'accès Internet. En ce qui concerne l'accès mobile à Internet, les possibilités techniques de blocage restent à créer. Les systèmes d'exploitation et les fabricants de terminaux mobiles ont un rôle décisif à jouer à cet égard.

Art. 96b Manipulation non autorisée d'installations de télécommunication (service de signalement)

Les cantons **AG**, **AI**, **AR**, **BE**, **BL**, **FR**, **GE**, **GL**, **LU**, **NW**, **OW**, **SO**, **TG**, **TI**, **VD**, **ZH**, la **CSSP**, l'**Assurance immobilière ZG**, **IVR**, **CAPO AI**, la **CCDJP**, la **CCPCS**, la **CG-MPS** et **SKS** demandent que les rôles de tous les services pour le processus global d'annonce et d'alarme dans le domaine cybernétique soient détaillés dans le rapport explicatif. **Suissedigital ainsi que,** à cet égard, **l'asut** et **Sunrise UPC** souhaitent que les efforts soient coordonnés et harmonisés au sein de l'administration avec d'autres projets législatifs relatifs à la sécurité.

Economiesuisse porte un jugement critique sur l'obligation d'exploiter un service de signalement, notamment parce qu'il vaudrait mieux se limiter à des principes d'action plutôt que d'imposer des prescriptions organisationnelles concrètes. Selon **Salt,** l'organisation du service de signalement devrait rester l'affaire de chaque fournisseur d'accès à Internet. Dans la perspective de la

collaboration entre l'OFCOM et le NCSC, il faudrait, selon **Swisscom,** fusionner l'actuel service de signalement avec celui qui est prévu pour les infrastructures critiques dans le cadre de la révision de la LSI.

Le canton **ZH** souhaite que soit défini plus précisément le délai fixé pour prendre les mesures de défense appropriées.

Art. 96c Manipulation non autorisée d'installations de télécommunication (exécution)

Salt se demande à quoi se réfère cette disposition d'exécution. **Swisscom** souhaite que les fournisseurs de services de télécommunication concernés soient consultés si d'autres exigences devaient être définies dans les PTA.

Art. 96d Sécurité des réseaux et des services exploités par les concessionnaires de radiocommunication mobile (application)

Le canton **ZG** souhaite que l'on examine si les mesures doivent s'appliquer à tous les services de téléphonie mobile, et non pas seulement à la cinquième génération.

Le canton **ZH** considère également qu'il n'est pas approprié de limiter le champ d'application des articles 96e-96g à la cinquième génération. Etant donné que ces prochaines années, les troisième et quatrième générations ainsi que les hotspots WiFi continueront d'être exploités par les opérateurs de téléphonie mobile en plus de la 5G, les dispositions devraient être formulées de manière technologiquement neutre.

Le canton **GE** pense qu'il faudrait appliquer cet article à toutes les générations actuelles et futures de téléphonie mobile.

Salt se demande également pourquoi les articles concernés ne devraient pas s'appliquer aux réseaux mobiles en général, et donc à toutes les générations.

Pour sa part, **Swisscom** estime que la limitation à la 5G est proportionnée et appropriée.

La **FER** rappelle que la 5G n'est que le vecteur de propagation: elle permettrait l'augmentation du vol de données et le chantage uniquement si les objets connectés sont faillibles, mal configurés, présentent des failles de sécurité potentielles ou que leur système de sécurité est immature au regard du risque connu. Tout cela rend l'exercice difficile et force le législateur à communiquer sur les méthodes de communication, le type de chiffrement, la protection adéquate et le niveau de sécurité attendu. Vaste chantier, qui dépasse clairement les limites fédérales, celui des fournisseurs d'accès et d'autres intermédiaires de communication et dont le débat se déplace au niveau des fournisseurs d'objets connectés et de leurs obligations, sans doute à travers des organes supra, tels l'IETF et leurs Best Current Practice, les accords de l'Organisation mondiale du commerce et de l'ENISA.

Art. 96e Sécurité des réseaux et des services exploités par les concessionnaires de radiocommunication mobile (gestion de la sécurité)

Al. 1

Sunrise et **Swisscom** ont déjà mis en place un système de gestion de la sécurité de l'information et, selon **Sunrise**, la sécurité doit être et rester de la responsabilité de chaque acteur.

Salt ne peut pas évaluer dans quelle mesure un tel système de gestion de la sécurité doit être mis en place. Toutefois, elle exploite déjà un système de gestion des risques, qui constitue un élément du système de gestion.

L'**asut** et **Salt** sont d'avis qu'une certification imposée représenterait des efforts et des coûts importants (uniques et récurrents) pour les petits fournisseurs. Une disposition concrète constituerait

une atteinte grave à la liberté économique. Il faut donc absolument laisser aux exploitants de réseau le soin de mettre en œuvre la gestion de la sécurité, et renoncer à prescrire des normes concrètes dans l'ordonnance et les PTA. L'OFCOM ne devrait intervenir qu'en cas d'incident, et examiner alors les faits conformément à l'art. 96g.

Al. 3

La **FER** et le canton **VS** soutiennent l'exigence de mettre en place un système de gestion de la sécurité de l'information basé sur les normes ISO. **Economiesuisse** est d'avis que le système de gestion exigé doit être accepté selon les normes et certifications courantes. Le marché a déjà créé des bases suffisantes dans ce domaine; une réglementation spécifique à la Suisse n'est pas appropriée.

Swisscom, **Sunrise** et la **FER** mentionnent la norme ISO/IEC 27001 comme référence pour le développement d'un système de gestion de la sécurité; **Swisscom**, **Salt**, le canton **VS** et la **FER** soutiennent le système de gestion de la continuité et la gestion des incidents de sécurité.

Sunrise exploite un système de gestion de la continuité des activités selon la norme ISO/IEC 22301. **Swisscom** et **Sunrise** mentionnent également cette norme comme référence pour l'élaboration d'un système de gestion de la continuité.

Art. 96f Sécurité des réseaux et des services exploités par les concessionnaires de radiocommunication mobile (exploitation des installations de télécommunication critiques)

Al. 1

L'**asut** approuve le projet, qui s'oriente pour l'essentiel vers des mesures également mises en œuvre dans d'autres pays (en particulier dans l'UE) et se base sur des normes et des initiatives de sécurité reconnues au niveau international (p. ex. ENISA, NESAS, GSMA knowledge base, SCAS, 3GGP, ISO). Renoncer dans une large mesure à une solution nationale particulière permet de mettre en œuvre les mesures efficacement et d'adapter en permanence les normes de sécurité aux évolutions techniques. En outre, les entreprises technologiques actives au niveau international ainsi que les clients commerciaux suisses s'orientent de plus en plus vers ces normes (p. ex. le secteur financier). Cette tendance engendre une augmentation de la sécurité du réseau dans tous les secteurs et montre en outre que le marché et la concurrence conduisent automatiquement à une augmentation du niveau de sécurité.

Swisscom fait savoir qu'elle applique déjà les normes de sécurité pertinentes établies au niveau international.

Salt salue la proposition de certification selon des normes de sécurité reconnues. Il s'agit d'éviter la création de normes spécifiques à la Suisse. Les réseaux de téléphonie mobile suisses sont considérés par l'Office fédéral pour l'approvisionnement économique du pays (OFAE) comme étant d'importance systémique et comme une infrastructure critique. Par conséquent, les installations de télécommunication correspondantes sont critiques en termes de sécurité. Salt ne voit donc pas bien ce que l'OFCOM devrait préciser à cet égard.

Al. 2

L'obligation de localisation proposée concernant les centres d'exploitation de réseau et de sécurité (Suisse, EEE Royaume-Uni) est approuvée par **IVR**, la **CCPCS**, la **CCDJP**, **SG**, **KAPO AI**, **GVZG**, les cantons **BE**, **OW**, **GE**, **GL**, **FKS**, **SO**, **VD**, **VS**, **ZH** et **Swisscom**. **Salt** souhaite étendre la réglementation aux Etats disposant d'une protection des données adéquate selon la liste du PFPDT. Outre leur accord sur l'obligation de localisation, **IVR**, la **CCPCS**, la **CCDJP**, **SG**, **KAPO AI**, **GVZG**, les cantons **BE**, **OW**, **GE**, **GL**, **FKS**, **SO** et **VD** proposent d'imposer également un siège social ou une filiale en Suisse.

Art. 96g Sécurité des réseaux et des services exploités par les concessionnaires de radiocommunication mobile (prescriptions applicables et surveillance)

Al. 1

L'**UDC** part du principe que la conception des PTA par l'OFCOM se fait en étroite collaboration avec la branche.

Selon l'**asut**, il faut éviter les réglementations spéciales pour la Suisse, car elles freinent le progrès technologique et la force d'innovation. Cela vaut également pour les PTA.

Sunrise UPC et **digitalswitzerland** estiment qu'il est juste que le projet s'oriente essentiellement vers des mesures de l'UE et des normes de sécurité reconnues au niveau international et qu'il ne prévoie pas de solution nationale particulière. Selon **Sunrise UPC**, cette orientation doit également être maintenue pour les PTA.

SUISSEDIGITAL est d'avis que l'implémentation et la mise en œuvre des mesures de sécurité doivent se baser sur l'expertise des fournisseurs de services de télécommunication et tenir compte de leurs activités.

Selon **Swisscom,** les opérateurs de téléphonie mobile appliquent déjà les normes de sécurité établies. Il faut renoncer à édicter des prescriptions spécifiques à la Suisse, au risque d'un manque d'harmonisation internationale. Pour les futures prescriptions techniques et administratives, les opérateurs concernés doivent être consultés, et les autres aspects de l'application et de la mise en œuvre discutés en étroite collaboration avec eux.

Salt demande la suppression de cet alinéa car, selon le choix des normes et des certifications correspondantes, une charge de travail importante et des coûts élevés pourraient survenir, en particulier pour les petits fournisseurs.

Al. 2

L'**UDC**, **Swisscom** et **economiesuisse** proposent de modifier la formulation de cet alinéa en précisant que l'OFCOM peut exiger un examen approprié en cas de "soupçon fondé", c'est-à-dire en cas de soupçon qualifié et non pas seulement de simple soupçon (voir p. ex. l'art. 9, al. 1, de la loi sur le blanchiment d'argent, l'art. 5 de l'ODiTr, etc.).

Salt estime que l'étendue d'un éventuel audit devrait être limitée aux installations de télécommunication concernées par un soupçon de violation du droit.

4 Autres remarques et propositions

La **CG-MPS**, **IVR**, la **CCPCS**, la **CCDJP**, la **KAPO AI**, **GVZG, CSSP,** les cantons **AR**, **BL**, **TG**, **SG**, **LU**, **NW**, **FR**, **BE**, **TI**, **ZG**, **OW**, et **SO** proposent, au sujet de la menace de cyberattaques contre des infrastructures critiques, de mettre également en évidence les tâches de l'armée et de les intégrer dans l'OST.

IVR, la **CCPCS**, la **CCDJP**, **GVZG**, **FKS**, la **KAPO AI**, les cantons de **SG**, **BE**, **OW**, **GE**, **GL**, **SO** et **VD** estiment que la révision de l'ordonnance devrait également améliorer la régulation des appels d'urgence (base de données des appels d'urgence, proxy LIS, routage dynamique). Enfin, selon le canton **FR,** il serait souhaitable que le Conseil fédéral présente une stratégie globale en matière de cybersécurité. Par ailleurs, la révision proposée devrait être régulièrement évaluée et, si nécessaire, complétée par des règles étatiques plus strictes.

Annexe : liste des participants et des abréviations

Cantons

AG	Canton d'Argovie
AI	Canton d'Appenzell Rhodes-Intérieures
AR	Canton d'Appenzell Rhodes-Extérieures
BE	Canton de Berne
BL	Canton de Bâle-Campagne
BS	Canton de Bâle-Ville
FR	Canton de Fribourg
GE	Canton de Genève
GL	Canton de Glaris
GR	Canton des Grisons
JU	Canton du Jura
LU	Canton de Lucerne
NE	Canton de Neuchâtel
NW	Canton de Nidwald
OW	Canton d'Obwald
SG	Canton de Saint-Gall
SH	Canton de Schaffhouse
SO	Canton de Soleure
TG	Canton de Thurgovie
TI	Canton du Tessin
UR	Canton d'Uri
VD	Canton de Vaud
VS	Canton du Valais
ZG	Canton de Zoug
ZH	Canton de Zurich

Partis politiques représentés à l'Assemblée fédérale

SPS / PSS	Sozialdemokratische Partei der Schweiz / Parti socialiste suisse
SVP / UDC	Schweizerische Volkspartei / Union Démocratique du Centre

Associations faîtières

USP	Union suisse des paysans
economiesuisse	

Autres participants

asut	Schweizerischer Verband der Telekommunikation / Association suisse des télécommunications
Centre Patronal	
digitalswitzerland	
FER	Fédération des entreprises romandes Genève
FKS	Coordination suisse des sapeurs-pompiers
GVZG	Assurance immobilière ZUG
IVR	Association Internet pour le sauvetage

KAPO AI	KAPO Appenzell Rhodes-Intérieures
CCDJP / CCDJP	Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren / Conférence des directrices et directeurs
KKPKS / CCPCS	Konferenz der kantonalen Polizeikommandanten der Schweiz / Conférence des commandants des polices cantonales de Suisse
RK MZF / CG-MPS	Regierungskonferenz Militär, Zivilschutz und Feuerwehr / Conférence gouvernementale des affaires militaires, de la protection civile et des sapeurs-pompiers
Salt Mobile SA	
SRG / SSR	Schweizerische Radio- und Fernsehgesellschaft / Société suisse de radiodiffusion et télévision
SUISSEDIGITAL	Verband für Kommunikationsnetze / Association de réseaux de communication
Sunrise	Sunrise UPC GmbH
Swisscom	Swisscom (Suisse) SA
WEKO / COMCO	Wettbewerbskommission / Commission de la concurrence