ETAT DE FRIBOURG
STAAT FREIBURG

Conseil d'Etat CE
Staatsrat SR

Rue des Chanoines 17, 1701 Fribourg

T +41 26 305 10 40, F +41 26 305 10 48
www.fr.ch/ce

Conseil d'Etat
Rue des Chanoines 17, 1701 Fribourg

PAR COURRIEL

Département fédéral de l'environnement, des transports,
de l'énergie et de la communication DETEC
Madame la Conseillère fédérale
Simonetta Sommaruga
Palais fédéral Nord
3003 Berne

Courriel : tp-secretariat@bakom.admin.ch

Fribourg, le 8 mars 2022

2022-200
Modification de l'ordonnance sur les services de télécommunication (OST)

Madame la Conseillère fédérale,

Nous vous remercions de nous avoir associés à la consultation sur la modification de l'ordonnance sur les services de télécommunication (OST). Le projet précité a retenu toute notre attention.

Le Conseil d'Etat salue la présente modification de l'OST qui vise à donner au Conseil fédéral des compétences accrues dans le domaine de la sécurité de l'information et des infrastructures et services de télécommunications. Les objectifs définis, à savoir lutter de manière plus efficace contre la manipulation non autorisée d'installations de télécommunication et garantir un haut niveau de sécurité dans l'exploitation de la dernière génération de réseaux de télécommunication (5G), revêtent une importance essentielle dans un contexte où la cybercriminalité devient un phénomène de plus en plus récurrent. Du point de vue sécuritaire, il est important de noter que les infrastructures de télécommunication font partie des infrastructures stratégiques critiques dont la protection demande la plus grande attention. Une importance particulière doit être accordée à la sécurisation des réseaux de télécommunication de dernière génération car les nouvelles applications concerneront probablement aussi des domaines sensibles tels que la finance, l'énergie ou encore la santé.

Enfin, les enjeux évoqués dans le rapport explicatif sont importants du point de vue économique. Les entreprises et notamment les PME font de plus de plus l'objet de cyberattaques qui occasionnent souvent des dégâts importants, tant sur le plan financier que réputationnel. L'identification des scénarios de risque et l'adoption de mesures de sécurité appropriées sont donc fondamentales pour éviter des dommages économiques considérables à l'avenir.

Partant de ce constat, le Conseil d'Etat soutient les mesures proposées car elles améliorent globalement la sécurité des informations et des infrastructures en matière de télécommunication. Il estime en outre que l'orientation du projet de modifications vers les standards internationaux en la matière est pertinente. Néanmoins, le Conseil d'Etat souhaite apporter les commentaires généraux suivants concernant le projet de modification de l'OST :

> *Approche transversale* : La lutte contre la cybercriminalité et la gestion des risques en la matière requièrent une approche globale et transversale qui tient notamment compte des questions de sensibilisation et de formation. On constate en effet qu'une partie relativement importante des PME n'est pas consciente des risques élevés en matière de cybercriminalité. De ce point de vue, il aurait été souhaitable que le Conseil fédéral soumette une stratégie globale en matière de cybersécurité et que les modifications légales proposées s'y réfèrent chaque fois, dans une perspective transversale. Or le rapport explicatif concernant la révision de l'OTS ne mentionne pas la manière dont la proposition s'inscrit dans une telle stratégie, et quelles autres mesures sont prévues afin de gérer les risques importants de manière globale.

> *Approche subsidiaire* : Le Conseil d'Etat constate que les mesures proposées reposent exclusivement sur l'action privée et en partie volontaire des prestataires en matière de services de télécommunication. Si cette approche se justifie dans l'optique de la subsidiarité, elle ne tient pas entièrement compte de l'importance stratégique du secteur et de l'évolution rapide des menaces en matière de cybercriminalité. Pour cette raison, le Conseil d'Etat est de l'avis qu'une action étatique plus décidée doit être possible si les analyses de risques révèlent une telle nécessité. Dans cette perspective, les mesures introduites dans le cadre de la présente révision doivent faire l'objet d'une évaluation régulière et, le cas échéant, être complétées par des obligations plus formelles.

> *Positionnement de la place économique suisse* : Le Conseil d'Etat saisit l'occasion pour souligner que la cybersécurité constitue de plus en plus un facteur de compétitivité et d'attractivité économique. La Suisse dispose d'avantages concurrentiels importants en la matière en raison de sa stabilité et de son excellente réputation sur le plan international quant à la qualité de ses services et infrastructures. Il est donc important d'exploiter davantage ce potentiel économique et de renforcer le positionnement de la Suisse. A cet égard, l'élaboration d'une stratégie transversale qui prend également en compte les aspects de promotion économique aurait été souhaitable, comme indiqué plus haut.

En outre, nous appuyons les modifications particulières suivantes.

> *L'intégration des organismes feux bleus et des infrastructures critiques dans les processus d'alarme et d'annonce doit être précisée* : Aujourd'hui en effet, plus de 70% des appels d'urgence sont passés au moyen d'appareils téléphoniques cellulaires. Il s'ensuit que les coupures des réseaux de téléphonie mobile ont des conséquences importantes. Elles ont des implications directes pour les appels d'urgence et pour la maîtrise des événements par les organismes feux bleus, de même que pour les exploitants d'infrastructures critiques, qui doivent pouvoir compter sur des réseaux de téléphonie mobile de la dernière génération qui soient fiables et sûrs.

> *Les rôles des différents acteurs et organes doivent être décrits dans le détail* : Pour améliorer le traitement et la diffusion des signalements de perturbations reçus, l'ordonnance révisée prévoit de renforcer le rôle de la Centrale nationale d'alarme (CENAL), attendu qu'elle exploite une infrastructure informatique sûre, 24 heures sur 24 (art. 96). Par contre, les cyberattaques doivent être annoncées à un service de signalement (art. 96b) devant encore être créé. Il existe en outre d'autres organisations qui s'occupent des cyber-attaques. Ainsi, le « National Cyber Security Center (NCSC) », la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) et les centrales d'alarme cantonales, par exemple, doivent être intégrés dans les activités. Pour cette raison, il n'est pas possible que seul l'OFCOM soit informé par la CENAL sur les signalements de perturbations reçus. Les rôles de tous les services au sein du processus global d'annonce et d'alarme dans le domaine cybernétique doivent être présentés dans le détail dans le rapport explicatif. La création d'un point de contact unique (SPOC) doit fondamentalement être visée pour simplifier la gestion des crises.

> *Les fournisseurs sont tenus d'annoncer sans délai les perturbations de l'exploitation de leurs installations et services de télécommunication si 30'000 clients sont potentiellement concernés par une panne qui durera plus de 15 minutes* : Le nombre de 30'000 clients potentiellement touchés correspond à une ville suisse de taille moyenne. Par conséquent, selon le projet soumis, une perturbation touchant l'ensemble du canton d'Appenzell Rhodes-Intérieures, qui compte 16'300 habitants, ne serait pas annoncée. Il est par ailleurs important que la durée de la perturbation soit évaluée. Actuellement, les organisations d'appels d'urgence considèrent comme étant problématiques les perturbations dont on peut s'attendre à ce qu'elles toucheront pendant plus de 15 minutes au moins 1'000 clientes et clients.

> *Les tâches de l'armée en relation avec les menaces contre les infrastructures critiques par des cyberattaques provenant d'Etats, et concernant la défense contre ces attaques, doivent être présentées et intégrées dans l'OST* : Depuis quelques années, on assiste à une renaissance de la politique de puissance classique. Aujourd'hui déjà, certains Etats utilisent régulièrement leurs moyens cybernétiques dans le sens d'une « guerre froide cybernétique ». En cas de conflit armé en Europe, il faut s'attendre à une utilisation à grande échelle de ces moyens, et des Etats qui ne seraient pas directement concernés par le conflit seraient vraisemblablement aussi touchés. Ces dernières années, l'armée a pris des mesures pour se préparer à un tel scénario. Ainsi, dans le domaine Défense, la Base d'aide au commandement (BAC) est responsable de la planification des actions, du suivi de la situation, de la maîtrise des événements et de la formation du personnel ainsi que des militaires dans l'espace cybernétique. Avec la poursuite du développement de l'armée (DEVA), une cybercompagnie a été constituée pour appuyer l'organisation professionnelle de la BAC. A partir de 2022, toutes les cyberformations de l'armée suisse seront intégrées dans le nouveau cyberbataillon 42. L'OST révisée doit tenir compte du rôle de l'armée et décrire les tâches de cette dernière.

En vous remerciant de nous avoir consultés, nous vous prions d'agréer, Madame la Conseillère fédérale, l'expression de nos respectueuses salutations.

Au nom du Conseil d'Etat :

Olivier Curty, Président

Olivier Curty
Signature électronique qualifiée · Droit suisse

Danielle Gagnaux-Morel, Chancelière d'Etat

Danielle Gagnaux-Morel
Signature électronique qualifiée · Droit suisse

L'original de ce document est établi en version électronique

Copie
—
à la Direction de l'économie, de l'emploi et de la formation professionnelle ;
à la Direction de la sécurité, de la justice et du sport ;
à la Chancellerie d'Etat.