Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS

Office fédéral de la cybersécurité OFCS

Berne, 27 novembre 2024

Projet d'ordonnance sur la cybersécurité (OCyS)

Consultation du 22 mai 2024 au 13 septembre 2024

Rapport sur les résultats de la consultation

Table des matières

1 Contexte

Le 22 mai 2024, le Conseil fédéral a adopté le projet d'ordonnance sur la cybersécurité (OCyS) et le rapport explicatif. Il a chargé le Département fédéral de la défense, de la protection de la population et des sports (DDPS) de mener une procédure de consultation. Celle-ci a duré du 22 mai 2024 au 13 septembre 2024. La liste de tous les participants à la consultation, avec les abréviations utilisées ci-après, se trouve en annexe.

69 prises de position ont été données :

69	**Total des avis reçus**
23	Gouvernements cantonaux
3	Conférences cantonales et commissions fédérales
4	Partis
2	Associations faîtières des communes et des villes œuvrant au niveau national
19	Associations œuvrant au niveau national
12	Entreprises concernées
7	Autres milieux concernés

Les prises de position sont mises en ligne sur la plateforme de publication du droit fédéral « Fedlex »[1].

2 Objet du projet soumis à consultation

Le 11 décembre 2020, le Conseil fédéral a chargé le Département fédéral des finances (DFF) d'élaborer les bases légales nécessaires à l'introduction d'une obligation de signaler les cyberattaques visant les infrastructures critiques. Le Conseil fédéral a ensuite adopté le 2 décembre 2022 le projet concernant ces bases légales et le message relatif à la modification de la loi du 18 décembre 2020 sur la sécurité de l'information (LSI)[2] établi à l'intention du Parlement. Ce dernier a ensuite approuvé les modifications de la LSI le 29 septembre 2023[3] ; le délai référendaire a expiré le 18 janvier 2024 sans avoir été utilisé.

Le projet d'ordonnance faisant l'objet du présent rapport contient d'une part les dispositions d'exécution du chapitre 5 de la LSI dans sa version révisée concernant l'obligation de signaler les cyberattaques menées contre les infrastructures critiques. D'autre part, il règle des aspects organisationnels en rapport avec la cybersécurité. Il est prévu que l'ordonnance entre en vigueur en même temps que le chapitre 5 révisé de la LSI le 1er janvier 2025.

La LSI est entrée en vigueur le 1er janvier 2024 – sans le chapitre révisé susmentionné concernant les tâches du nouvel Office fédéral de la cybersécurité (OFCS) et l'obligation de signaler les cyberattaques visant les infrastructures critiques. L'ordonnance du 27 mai 2020 sur les cyberrisques (OPCy)[4] a également été abrogée à cette date[5]. Les dispositions qu'elle contenait ont été en partie transférées dans la LSI révisée (notamment les définitions). Les dispositions de l'OPCy qui portaient sur la sécurité informatique de la Confédération ont été reprises dans l'ordonnance du 8 novembre 2023 sur la sécurité de l'information (OSI)[6]. Les tâches du Centre national pour la cybersécurité (NCSC) définies dans l'OPCy – notamment celles relatives à l'économie et à la population – ne sont pas ancrées dans l'OSI, car la révision de la LSI leur donne une nouvelle base légale. Par ailleurs, le NCSC a été transféré à l'OFCS au sein du DDPS le 1er janvier 2024. Pour cette raison, des dispositions organisationnelles sur l'OFCS figurent à l'art. 15*a*, al. 1

1 www.fedlex.admin.ch > Consultations > Consultations terminées > 2024 > DDPS
2 RS **128**
3 FF **2023** 2296
4 RS **120.73**
5 RO **2023** 735 (annexe 2, ch. I)
6 RS **128.1**

et 2, let. a à g, de l'ordonnance du 7 mars 2003 sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports (Org-DDPS)[7].

L'ordonnance faisant l'objet du présent rapport précise et décrit plus concrètement les tâches de l'OFCS, ainsi que l'obligation de signaler les cyberattaques contre les infrastructures critiques. Elle porte donc surtout sur les relations entre l'OFCS et les parties assujetties hors administration fédérale, tandis que l'OSI définit les tâches et les compétences relatives à la sécurité de l'information au sein de l'administration fédérale.

3 Résultats de la consultation

3.1 Appréciation globale du projet

L'OCyS reçoit globalement un écho positif. Les prises de position sont pour la plupart favorables à l'initiative pour le renforcement de la cybersécurité en Suisse. De nombreux acteurs saluent par ailleurs les efforts visant à améliorer la sécurité dans ce domaine.

Malgré l'approbation générale, les critiques constructives et les propositions d'amélioration sont nombreuses. Elles se réfèrent souvent à des aspects spécifiques de l'ordonnance et ont pour objectif d'en améliorer le caractère pratique et l'efficacité.

L'harmonisation et la coordination des différentes procédures de signalement, tout comme la précision de certains termes et processus et l'adaptation des obligations de signaler, sont considérées comme prioritaires afin d'éviter une charge administrative disproportionnée. Les participants à la consultation ont également demandé de mieux tenir compte de la collaboration avec les autorités de poursuite pénale et d'assouplir les délais et les exceptions.

Différents secteurs, tels que le secteur financier, le secteur de la santé et celui des télécommunications, expriment en outre des préoccupations spécifiques à leurs branches, celles-ci reflétant leurs besoins et défis respectifs.

Dans une perspective fédérale, les cantons soulignent que la collaboration entre la Confédération et les cantons est nécessaire tout comme la prise en compte des structures cantonales.

Les aspects économiques ont aussi leur importance. Bien qu'elles soutiennent en principe l'ordonnance, les associations économiques et les entreprises appellent à la proportionnalité et demandent des solutions économiquement viables.

Dans l'ensemble, un large consensus s'est dégagé sur la nécessité d'adopter l'OCyS. Les participants à la consultation sont d'avis que sa mise en œuvre requiert néanmoins des précisions et des ajustements au niveau de la pratique.

3.2 Prises de position groupées concernant l'OCyS en fonction de l'évaluation et de l'orientation

3.2.1 Aperçu des réponses positives recueillies dans le cadre de la consultation sur l'OCyS sans propositions de modification significatives

L'OCyS a été approuvée sans réserve par certains participants à la consultation :

– Plusieurs *cantons* ont émis un avis particulièrement positif (*BS, OW, SZ, SG, NW* et *TI*).

7 RS **172.214.1**

- Du côté des *exploitants d'infrastructures*, *Transitgas AG* accueille favorablement l'ordonnance, la considérant comme une étape importante pour garantir la sécurité des infrastructures critiques. *RAILplus* a également mentionné que le texte répondait aux attentes et n'a pas eu de commentaires significatifs. *La FAMH* est favorable à l'OCyS. Elle fait remarquer que tous les laboratoires médicaux ne sont pas concernés par l'obligation de signaler en cas de cyberattaques et recommande à ses membres de faire des signalements volontaires, même s'ils ne tombent pas sous le coup de la définition légale.

3.2.2 Évaluation positive contenant des propositions d'amélioration ou des observations

L'OCyS a reçu un accueil majoritairement positif. De nombreux participants à la consultation ont donné leur accord de principe accompagné de propositions d'améliorations ou d'observations :

- Un large soutien s'est manifesté au *niveau cantonal*. Les cantons de *AG, BE, FR, GE, GL, GR, LU, SH, SO, UR, VD, VS, ZG* et *ZH* ont salué l'ordonnance tout en formulant certaines demandes. Ils ont par exemple proposé des améliorations concernant les exceptions à l'obligation de signaler (*AG*) et souhaité des précisions et une meilleure prise en compte de la chaîne logistique (*ZH*).

- Certaines *autorités fédérales* telles que *le MPC* et *le BFC* ont soutenu le principe de l'ordonnance, mais ont demandé de mieux tenir compte de la collaboration avec les autorités de poursuite pénale ou de limiter la charge de travail relative aux signalements initiaux.

- Plusieurs *partis politiques* comme *Le Centre, le PLR* et *le PS* ont approuvé l'ordonnance en indiquant cependant de prêter attention à différents aspects : *Le Centre* a souligné la nécessité de structures nationales fortes et *le PLR* a mis en garde contre une charge administrative disproportionnée.

- Des *associations et groupes d'intérêts* tels que *l'asut, l'AES, CH++, digitalswitzerland, economiesuisse, ISSS, Pour Demain, l'USAM, Swiss Banking, Swiss FS-CSC, SwissICT, Swico, SUISSEDIGITAL, scienceindustries, l'UVS, l'ACS, H+, NEDIK, la CMP, CH++, swissuniversities, le PNR 77/EPFZ/UNIL* et *eAVS/AI* ont également largement soutenu l'ordonnance tout en attirant l'attention sur les potentiels d'amélioration. Ils ont souvent relevé la nécessité d'une harmonisation avec les réglementations existantes et demandé des délais plus souples et des adaptations qui tiennent mieux compte de la pratique.

- *Les entreprises et les exploitants d'infrastructures* comme *l'aéroport de ZH, FER, Primeo, Migros, les CFF, la Poste CH SA, Sunrise, la SUVA, Salt, Swissgrid* et *Switch* ont aussi salué l'ordonnance, mais ont parfois exprimé des préoccupations spécifiques à leur branche. Ils ont ainsi demandé des précisions relatives à l'obligation de signaler et ont porté un regard critique sur la complexité de l'ordonnance et les processus de signalement non harmonisés.

Bien que largement approuvée, l'OCyS présente aussi un potentiel d'amélioration dans de nombreux domaines. Les commentaires les plus fréquents se rapportent à un besoin de précisions, à l'harmonisation avec les réglementations existantes, à la prise en compte des besoins spécifiques des branches et à la garantie d'une mise en œuvre proche de la pratique et économiquement justifiable.

3.2.3 Évaluation neutre ou mixte

Dans le cadre de la consultation sur l'OCyS, certains participants se sont montrés neutres ou mitigés en se positionnant de manière prudente ou ciblée :

- *L'aéroport de GE* a adopté une position neutre et ne s'est pas prononcé sur le contenu de l'ordonnance. Il n'a pas émis de commentaire spécifique et s'est seulement exprimé sur les adaptations de processus prévues.

- *La CCDJP* a opté pour un point de vue neutre en renonçant à se positionner sur le contenu de l'ordonnance et en laissant aux différents cantons le soin de se prononcer sur le projet.

- *Le Parti Pirate Suisse* n'émet aucun jugement de valeur concernant l'OCyS. Il se concentre dans sa prise de position sur une préoccupation principale en lien avec la divulgation coordonnée des vulnérabilités.

- *L'ASIP* s'est positionnée de manière très ciblée et s'est exprimée exclusivement sur l'exception à l'obligation de signaler pour la branche qu'elle représente.

3.3 Propositions et remarques sur l'avant-projet

3.3.1 Remarque préliminaire

Les remarques, propositions de modification et critiques concernant les différentes dispositions du projet de l'OCyS sont présentées ci-dessous. Seuls sont mentionnés les principaux arguments avancés par prise de position. Les prises de position particulièrement détaillées ne sont reprises que dans la mesure où elles demandent des modifications matérielles concrètes. Pour plus de détails, il est possible de consulter les prises de position publiées sur internet.

Le présent rapport ne mentionne pas les consentements tacites ou l'absence de réaction au sujet d'un article. Toutefois, le lecteur ne doit pas oublier qu'une majorité des participants à la consultation approuve en principe une grande partie des dispositions proposées dans l'ordonnance malgré les nombreux commentaires que certaines dispositions ont suscités. Aucun avis n'a été donné sur la structure de l'ordonnance en tant que telle.

3.3.2 Propositions et remarques concernant les dispositions

3.3.2.1 Art. 1 (Objet)

Art. 1

La présente ordonnance règle :

a. la Cyberstratégie nationale et son comité de pilotage;

b. les tâches de l'Office fédéral de la cybersécurité (OFCS);

c. l'échange d'informations entre l'OFCS et les autorités ou organisations chargées de la protection contre les cyberincidents et les cybermenaces;

d. l'obligation de signaler les cyberattaques.

Le présent article a fait l'objet de trois prises de position qui se concentrent essentiellement sur la précision du champ d'application et la délimitation par rapport à d'autres réglementations :

- *La FER* souligne l'absence de réglementation en matière de cyberdéfense.

- *BL* demande que le Réseau national de sécurité (RNS) soit pris en compte.

- *BE* souhaite qu'une distinction claire soit faite entre les tâches de l'OFCS spécifiques à l'OCyS et les tâches générales mentionnées dans l'OSI.

3.3.2.2 Art. 2 (Cyberstratégie nationale)

Art. 2 Cyberstratégie nationale
[1] La cyberstratégie nationale (CSN) fixe le cadre stratégique de la prévention dans le domaine de la cybersécurité, de la détection précoce des cybermenaces ainsi que des possibilités de réaction et de la résilience en cas d'incident, ainsi que de la lutte contre la cybercriminalité.
[2] Elle est définie en accord avec les cantons.

Le champ d'application proposé a donné lieu à treize réactions.

❖ **Élargissement de la prise en compte des parties prenantes**

- *L'asut, Salt* et *Switch* demandent d'impliquer l'économie, la science et la société civile dans l'élaboration de la CSN et de modifier par conséquent l'art. 2, al. 2, comme suit : « Elle est définie en accord avec les cantons et avec la participation de l'économie, de la science et de représentants de la société civile. ».

- *ZG* et *Swissgrid* désapprouvent le fait que d'autres groupes d'intérêts, notamment les exploitants d'infrastructures critiques, n'aient pas été associés à l'élaboration de la CSN.

- *sgv/usam* souhaite que les représentants des communes participent à l'élaboration de la CSN.

- *L'UVS* déplore le manque d'implication des grandes villes et communes dans l'élaboration de la CSN.

❖ **Rôle et implication des autorités et des organisations spécifiques**

- *BL* demande de compléter le rapport explicatif et d'y préciser que les efforts avec la CSN doivent se faire en étroite collaboration avec les cantons.

- *UR* souligne l'importance du RNS. Ce dernier devrait ainsi continuer à collaborer de manière déterminante à la future création de la CSN.

- *ZH* souhaite que la « lutte contre la cybercriminalité » garantisse le recours au ministère public et à la police en tant qu'autorités compétentes.

- *La Poste CH SA* propose de tenir compte des représentants des infrastructures critiques et de les intégrer dans la composition de la CSN. Elle estime que la formulation « représentants de l'économie » n'est pas assez claire à cet égard.

❖ **Ajouts de contenu et critiques**

- *ISSS* désapprouve le fait que la collaboration internationale ne soit pas mentionnée dans le texte de l'ordonnance, vu que celle-ci joue un rôle important dans le cadre de la CSN.

- *Les CFF* demandent que l'« identification des menaces » (« Identity ») soit ajoutée à l'énumération de l'art. 2, al. 1, afin de couvrir les cinq fonctions du NIST Cybersecurity Framwork.

- *L'ASA* doute que la LSI constitue une base suffisante pour l'adoption des art. 2 ss P-OCyS.

❖ **Évaluations positives**

- *ZH* approuve la définition coordonnée de la CSN.

- *Swico* se réjouit du cadre stratégique central fixé pour la prévention, la détection précoce et la réaction aux cybermenaces.

3.3.2.3 Art. 3 (Instauration et organisation du comité de pilotage)

Art. 3 Instauration et organisation du CP CSN
[1] Le Conseil fédéral instaure un comité de pilotage de la Cyberstratégie nationale (CP CSN).
[2] Le CP CSN dispose d'un secrétariat, exploité par l'OFCS.

Deux participants à la consultation ont exprimé leur soutien à la mise en place et à l'organisation du CP CSN.

❖ **Soutien au CP CSN**

- *ISSS* et *la Poste CH SA* soutiennent la mise en place du CP CSN.

3.3.2.4 Art. 4 (Composition du CP CSN)

Art. 4 Composition du CP CSN
[1] Le CP CSN se compose de représentants des départements, de la Chancellerie fédérale, des cantons, de l'économie, de la société et des hautes écoles.
[2] Le Conseil fédéral désigne tous les cinq ans les membres du CP CSN, à l'exception des représentants des cantons, qui sont nommés par la Conférence des gouvernements cantonaux.
[3] Il nomme un président parmi les représentants de l'économie, de la société et des hautes écoles.

27 participants à la consultation se sont exprimés sur la composition du CP CSN.

❖ **Art. 4, al. 1**

- *CH++* salue la composition diversifiée du CP CSN. Elle souhaite toutefois des critères de sélection clairs pour les membres et une représentation adéquate des experts en sécurité.

- *Swiss Banking* et *Swiss FS-CSC* proposent de supprimer les mots « de la société » dans le texte de l'ordonnance.

- *economiesuisse* et *scienceindustries* désapprouvent le fait que la composition du CP ait été définie de façon autant anticipée. Ils demandent, tout comme *digitalswitzerland, l'aéroport de ZH, H+, ISSS, VS, Primeo, Swiss Banking, Swiss FS-CSC, l'AES, la Poste CH SA, l'ASA* et *Swissgrid*, d'inclure des représentants d'infrastructures critiques au sein du CP CSN et d'adapter en conséquence le texte de l'ordonnance.

- *L'aéroport de ZH* accueille favorablement la prise en compte de l'économie dans la composition du CP CSN et propose d'en être le représentant.

- *BL* souhaite des précisions sur la composition du personnel et l'intégration de représentants des communes et des infrastructures critiques dans le CP CSN.

- *FR* propose une représentation obligatoire du secteur de l'énergie au sein du CP CSN.

- *GE* suggère de compléter « société » par « civile » à l'art. 4, al. 1, afin de mieux refléter l'intention de représenter les intérêts des citoyens.

- *VD* et *l'ACS* recommandent d'inclure des représentants des communes dans le CP CSN.

- *Migros* propose que le CP CSN soit composé de sorte que les entreprises importantes, qui jouent un rôle essentiel dans l'approvisionnement du pays en biens et en services, soient représentées directement et non par le biais d'associations.

- *Les CFF* désapprouvent le manque d'informations relatives à la taille et à la composition du CP CSN. Ils demandent que les termes génériques tels que « économie » soient précisés afin de garantir une représentation adéquate des branches concernées.

- *sgv/usam* souhaite être directement représentée au sein du CP CSN.

- *L'UVS* déplore que les villes et les communes ne soient pas représentées au sein du CP CSN.

- *Swico* trouve que la composition diversifiée du CP CSN est conforme à l'objectif et propose d'inclure explicitement le secteur des TIC et de l'internet.

- *swissuniversities* offre son soutien pour rechercher une représentation adéquate des hautes écoles au sein du CP CSN et fait remarquer qu'il convient à cet égard de clarifier le rôle de *Switch.*

- *Le Centre* salue la composition équilibrée du CP CSN.

❖ **Art. 4, al. 2**

- *Swiss Banking* et *Swiss FS-CSC* proposent d'amener un complément d'information à l'art. 4, al. 2, relatif à l'expérience ou aux connaissances appropriées dans le domaine cyber : « Il faut veiller à ce que les personnes désignées pour être membres du CP CSN disposent d'une expérience ou de connaissances appropriées dans le domaine cyber. ».

❖ **Art. 4, al. 3**

- *GE* propose de compléter « société » par « civile » à l'art. 4, al. 1 et 3, afin de mieux refléter l'intention de représenter les intérêts des citoyens.

- *Swissgrid* demande de mentionner explicitement que les exploitants d'infrastructures critiques sont susceptibles d'assurer la présidence.

3.3.2.5 Art. 5 (Tâches du CP CSN)

Art. 5 Tâches du CP CSN Le CP CSN assume les tâches suivantes: a. il contrôle la CSN au moins une fois tous les cinq ans, il contribue à son développement et, au besoin, élabore des propositions visant à l'adapter; b. il élabore, en accord avec les acteurs cités dans la CSN, des propositions concernant les priorités et les calendriers de la concrétisation des mesures de la CSN; c. il évalue régulièrement la concrétisation des mesures et informe le Conseil fédéral et les cantons de tout retard; d. il soumet au besoin au Conseil fédéral des propositions visant à compléter les mesures; e. il établit, à l'intention du Conseil fédéral, des cantons et du public, un rapport annuel sur la concrétisation de la CSN.

Dix participants à la consultation se sont exprimés sur les tâches du CP CSN. L'al. 1, let. a, relatif à la périodicité des contrôles de la CSN a suscité le plus de réactions.

❖ **Propositions générales et compléments**

- *SH* et *le PNR 77/EPFZ/UNIL* demandent tous deux un *élargissement des compétences du CP CSN*. *SH* suggère ainsi d'ajouter une disposition d'urgence à l'art. 5 pour que le CP CSN soit habilité à prendre immédiatement les mesures appropriées en cas d'urgence et qu'il ne se limite pas à la seule élaboration de propositions et de calendriers. *Le PNR 77/EPFZ/UNIL* recommande de préciser également que le CP CSN a la compétence de veiller à la cohérence et à la mise en œuvre du CSN.

- Certains participants souhaitent une *amélioration de la coordination. ZG* propose des consultations régulières entre le CP CSN et les cantons. Dans ce contexte, *le PNR 77/EPFZ/UNIL* exige une meilleure coordination entre les acteurs de la CSN et une harmonisation avec d'autres stratégies nationales.

- *Le PNR 77/EPFZ/UNIL* demande une précision *des aspects organisationnels* en rapport avec l'art. 5 : l'organigramme et le statut de l'OFCS devraient être clarifiés et les compétences des autres services éventuellement spécifiées.

❖ **Art. 5, let. a (intervalle des contrôles de la CSN)**

- De nombreux participants estiment que l'*intervalle de contrôle* prévu par l'ordonnance est trop long. *ISSS* et *Le Centre* trouvent que l'intervalle de cinq ans est trop long, mais ne précisent pas à combien d'années il faudrait le réduire. *Les CFF* demandent un contrôle annuel assorti d'un examen détaillé tous les deux ans. *UR* souhaite qu'un contrôle ait lieu au moins tous les trois ans et *l'aéroport de ZH* au minimum tous les quatre ans.

- Dans leurs prises de position, certains participants ont également formulé des propositions relatives au *type de contrôle*. Ainsi, *ISSS* demande que l'on prévoie des ajustements supplémentaires basés sur l'analyse des risques et sur les circonstances. *GE* propose de remplacer « contrôle » par « audite » à l'art. 5, let. a afin de suggérer un examen plus détaillé et plus précis.

3.3.2.6 Art. 6 (Demande de renseignements sur les titulaires)

Art. 6 Demande de renseignements sur les titulaires
L'OFCS peut, afin d'avertir les autorités, les organisations ou les personnes d'une cybermenace imminente ou d'une cyberattaque en cours, requérir les coordonnées des titulaires de noms de domaine auprès du registre des noms de domaine relevant de la compétence de la Confédération ou qui sont subordonnés à ceux-ci.

Trois participants à la consultation se sont prononcés favorablement sur cet article. Ils ne souhaitent que des adaptations au niveau du texte :

- *GE* suggère de clarifier l'intention et le but de la demande de coordonnées des titulaires de noms de domaine en reformulant l'art. 6 de la manière suivante : « L'OFCS peut, afin d'avertir les autorités, les organisations ou les personnes visées par une cybermenace, imminente ou en cours, requérir les coordonnées des titulaires de noms de domaine auprès du registre des noms de domaine relevant de la compétence de la Confédération. ».

- *SH* se réjouit que l'OFCS soit habilité à interroger les titulaires des noms de domaine, tel que mentionné à l'art. 6. Il propose toutefois que l'OFCS puisse également bloquer les domaines criminels et qu'il ne se limite pas à émettre des avertissements.

- *ISSS* fait remarquer que l'OFCS ne possède pas les compétences nécessaires pour effectuer des recherches sur les titulaires à la suite d'attaques et pour obtenir des informations antérieures sur les titulaires.

3.3.2.7 Art. 7 (Analyse technique des cyberincidents et des cybermenaces)

Art. 7 Analyse technique des cyberincidents et des cybermenaces
[1] L'OFCS gère l'équipe nationale d'intervention en cas d'urgence informatique *(Computer Emergency Response Team [CERT]*), qui assume notamment des tâches suivantes: a. elle gère les incidents techniques; b. elle analyse les questions techniques; c. elle identifie et évalue les cybermenaces. [2] Il exploite une infrastructure résiliente et fonctionnant indépendamment du reste de l'informatique fédérale pour analyser les cyberincidents et les cybermenaces.

Seize participants à la consultation se sont exprimés sur cette disposition. Ils demandent surtout des modifications relatives au texte ou des clarifications.

❖ **Art. 7, al. 1 : analyse technique et CERT**

- S'agissant de la *définition et des tâches de la CERT, CH++* fait remarquer qu'il faudrait utiliser le terme « CSIRT » au lieu de « CERT », l'abréviation « CERT » faisant référence à une marque déposée. *Le BFC* suggère de préciser la composition de la CERT dans le rapport explicatif. Il propose aussi de remplacer, à l'art. 7, al. 1, let. a, les termes « incidents techniques » par « incident dans le domaine de la cybersécurité. ». La même remarque vaut pour la let. b. *ISSS* désapprouve le fait qu'aucune réglementation n'indique à qui s'adresse la CERT. Il relève que les let. a et b se concentrent sur la technique, contrairement à la let. c. Il souhaite en outre que l'article soit repensé, la directive complétée et les analyses publiées de manière générale. Enfin, *Pour Demain* propose de compléter l'art. 7, al. 1, let. a, par la « gestion des incidents techniques, y compris les événements sans intervention extérieure. ». Il suggère par ailleurs d'ajouter une let. d à l'al. 1 afin d'élargir le nombre des tâches prises en charge par la CERT et de mentionner qu'elle assume le monitoring des incidents liés à l'intelligence artificielle.

- Considérant la *collaboration et la coordination, economiesuisse* et *scienceindustries* recommandent une précision commune des prestations et de la collaboration entre l'OFCS, les CERT privées et les infrastructures critiques. *Swiss Banking* et *Swiss FS-CSC* trouvent qu'il est important de soutenir la gestion technique des incidents également à la demande d'autres autorités et organisations. Ils estiment par conséquent qu'il est indiqué de compléter l'art. 7, al. 1, let. a, par la proposition subordonnée suivante : « lorsque cela est nécessaire, également à la demande d'autres autorités et organisations ». *La CMP* constate que la collaboration avec les autorités de poursuite pénale n'est pas explicitement mentionnée. Elle propose donc d'ancrer les contacts avec ces autorités dans l'ordonnance. *Switch* demande pour sa part d'y fixer les échanges de la CERT avec des centres de compétence nationaux et internationaux. *Swissuniversities* recommande de régler dans l'ordonnance la collaboration entre la CERT de l'OFCS, la CERT de Switch et les organisations de cybersécurité des hautes écoles. Enfin, *l'AES* encourage une clarification commune des prestations et la collaboration entre l'OFCS, les CERT privées et les infrastructures critiques.

- Concernant la question des *ressources et de l'infrastructure, VS* recommande de partager les infrastructures ou les ressources avec d'autres organisations fédérales.

❖ **Art. 7, al. 2 : infrastructure**

- *CH++* estime que le terme « résiliente », mentionné à l'art. 7, al. 2, n'est pas assez précis et propose de le clarifier par la formulation suivante : « L'exploitation de cette infrastructure doit pouvoir être assurée à tout moment et si possible indépendamment de tiers. ». *CH++* soulève en outre la question de l'infrastructure technique pour les analyses et recommande de préciser l'utilisation des services Cloud.

- *L'aéroport de ZH* est favorable à l'indépendance de l'infrastructure de l'OFCS par rapport au reste de l'informatique fédérale et conseille d'avoir un niveau de protection élevé.

❖ **Autres observations**

- *eAVS/AI* souhaite que le rapport explicatif décrive plus clairement l'aide immédiate apportée par l'OFCS.

- *GE* propose de remplacer « qui » par « laquelle » dans la version française de l'art. 7, al. 1, afin d'éviter toute ambiguïté.

- *La CMP* recommande également de définir l'objet, les objectifs d'efficacité et l'étendue des « contremesures » et de décrire les compétences nécessaires de la CERT à cet effet.

3.3.2.8 Art. 8 (Priorités pour les conseils et l'assistance en cas de cyberattaque)

Art. 8 Priorité pour les conseils et l'assistance en cas de cyberattaque
[1] Si, en cas de cyberattaque, les demandes de conseils et d'assistance dépassent les capacités de l'OFCS, celui-ci peut alors établir des priorités pour leur traitement en fonction de l'urgence et de l'étendue des conseils et de l'assistance.
[2] Il prend alors en compte les impératifs de la sécurité et de l'ordre publics, du bien-être de la population et du fonctionnement de l'économie.

Douze participants à la consultation se sont exprimés sur cette disposition.

❖ **Observations générales sur l'art. 8**

- S'agissant de la *collaboration et des compétences* réglées par cette disposition*, le BFC* se demande s'il faut prévoir de faire appel à des fournisseurs de prestations privés en cas de crise grave et si l'on pourrait, le cas échéant, définir au préalable les critères pour les identifier et les sélectionner. *ZH* recommande de formaliser la collaboration avec le ministère public et la police et d'associer les autorités cantonales. Dans ce contexte*, Switch* demande de concrétiser la subsidiarité de l'OFCS et de définir la responsabilité individuelle des exploitants privés. Enfin*, swissuniversities* suggère que *Switch* décharge l'OFCS en cas de cyberattaques visant les hautes écoles.

- Concernant les *compétences et les mesures* de cette disposition*, ISSS* propose de permettre un renforcement externe de la CERT en cas de cyberattaque. *ZH* recommande pour sa part de fixer dans le texte de l'ordonnance l'objet, les objectifs d'efficacité et l'étendue des « contre-mesures » et de décrire les compétences de la CERT.

- Considérant le rôle de l'OFCS*, eAVS/AI* mentionne que l'art. 8 s'applique, concernant la priorisation, lorsqu'il s'agit de recueillir des informations supplémentaires en cas d'incident de sécurité. *Les CFF* suggèrent de clarifier le lien entre le signalement et la demande d'assistance. *Swico* se réjouit que l'OFCS soit chargé des conseils et de l'assistance. Il met toutefois en garde contre le risque que les prestations étatiques entrent en concurrence avec les offres privées en cas d'attaque de faible priorité.

❖ **Art. 8, al. 1 : priorités et critères**

- *digitalswitzerland* souhaite une liste de critères spécifiques et une gradation des scénarios de dommages concrets afin *d'établir les priorités*. *GE* propose de compléter les critères de gestion des priorités. *UR* recommande de classer les entreprises et les organisations soumises à l'obligation de signaler par ordre de priorité, selon leurs fonctions. *Les CFF* demandent quant à eux de procéder à une priorisation claire en cas de manque de capacité. Enfin, *l'AES* souhaite que les critères de priorités soient définis avec transparence, sur la base de la liste des infrastructures critiques de l'Office fédéral de la protection de la population (OFPP).

- En ce qui concerne la *communication des priorités, GE* propose de créer un al. 3 qui prévoirait ce qui suit : « Il communique alors aux parties concernées les priorités définies. ».

❖ **Art. 8, al. 2 : prise en compte des intérêts publics**

- À propos de l'art. 8, al. 2, *Digitalswitzerland* fait observer qu'une liste des critères spécifiques ou qu'une gradation des scénarios de dommages concrets pour l'établissement des priorités constituerait une aide importante pour l'économie numérique.

3.3.2.9 Art. 9 (Divulgation coordonnée des vulnérabilités)

Art. 9 Divulgation coordonnée des vulnérabilités

[1] L'OFCS veille à coordonner la divulgation des vulnérabilités selon les normes internationales reconnues.

[2] Il fixe au fabricant du matériel informatique ou du logiciel concerné un délai de 90 jours pour éliminer les vulnérabilités.

[3] Il peut raccourcir ce délai si la vulnérabilité:

a. met en péril le fonctionnement d'infrastructures critiques;

b. peut être très facilement exploitée pour une cyberattaque, ou

c. touche des systèmes très répandus.

[4] Il peut prolonger le délai lorsque l'élimination de la vulnérabilité s'avère particulièrement complexe.

[5] Il peut informer les exploitants d'infrastructures critiques de la présence de vulnérabilités avant même l'élimination ou la divulgation de celles-ci.

[6] Les al. 1 à 4 ne s'appliquent pas aux vulnérabilités découvertes par l'Office fédéral de la communication (OFCOM) dans le cadre de ses contrôles de surveillance (art. 36 ss de l'ordonnance du 25 novembre 2015 sur les installations de télécommunication). Dans de tels cas, l'OFCOM informe l'OFCS.

[7] L'OFCS peut informer immédiatement l'OFCOM des vulnérabilités dans les installations de télécommunication selon à l'art. 3, let. d, de la loi du 30 avril 1997 sur les télécommunications.

Cet article a suscité de nombreuses réactions. 25 participants à la consultation se sont exprimés sur la divulgation coordonnée des vulnérabilités.

❖ **Observations générales sur l'art. 9**

- Concernant la *définition et la gestion des vulnérabilités, SH* fait remarquer de manière générale qu'il faut donner aux fabricants un délai d'élimination des vulnérabilités suffisant avant de les rendre publiques. *Swiss Banking*, *Swiss FS-CSC* et *les CFF* demandent de définir le terme « vulnérabilité ». *Les CFF* souhaitent par ailleurs des clarifications relatives aux délais d'élimination des vulnérabilités, à la communication entre l'OFCS et l'Office fédéral des transports (OFT), à la délimitation de l'obligation de signaler entre fabricants et exploitants et au lien entre fabricants et exploitants.

- *Le Centre* considère que le *rôle et les tâches de l'OFCS* sont appropriés et nécessaires.

- *Le PNR 77/EPFZ/UNIL* recommande de concrétiser, au niveau de l'ordonnance, les conséquences en cas de non-élimination.

- *SwissICT* craint une charge de travail supplémentaire pour les fabricants et exprime des réserves par rapport aux risques liés à la confidentialité.

❖ **Art. 9, al. 1 : principe de la divulgation coordonnée**

- *Le PS* approuve expressément la réglementation et y voit une nette amélioration par rapport à la situation actuelle.

- *L'asut, Salt, digitalswitzerland* et *ZG* proposent que le texte de l'ordonnance tienne compte des meilleures pratiques en plus des normes internationales. *L'asut, Salt et digitalswitzerland* conseillent de formuler l'art. 9, al. 1, de la manière suivante : « [1] Après leur élimination, l'OFCS veille à coordonner la divulgation des vulnérabilités selon les normes internationales reconnues et les meilleures pratiques. ». *ZG* demande également d'élargir le champ d'application aux exploitants et aux services.

- *BE* suggère de rédiger l'al. 1 comme suit : « [1] L'OFCS veille à coordonner la divulgation des vulnérabilités. ».

- En ce qui concerne le moment de la divulgation, *economiesuisse* et *scienceindustries* proposent qu'elle n'ait lieu qu'une fois les vulnérabilités éliminées.

❖ **Art. 9, al. 2 : délai d'élimination des vulnérabilités**

- *digitalswitzerland, l'asut, Salt, economiesuisse, scienceindustries* et *Swico* souhaitent un *assouplissement du délai. economiesuisse, scienceindustries* et *Swico* proposent de mentionner dans le texte de l'ordonnance un « délai raisonnable » au lieu du « délai de 90 jours », jugé rigide. *L'asut et Salt* demandent toutefois que l'on précise que le délai raisonnable doit être d'au moins 90 jours.

- S'agissant de la *spécification des destinataires, H+* propose de préciser qu'il s'agit de fabricants de matériel informatique ou de logiciels des infrastructures critiques. *SwissICT* demande pour sa part d'ajouter les exploitants en tant que personnes potentiellement tenues d'éliminer les problèmes.

❖ **Art. 9, al. 3 : information en cas de cybermenace aiguë**

- *BE* recommande de formuler l'art. 9, al. 3, comme suit pour une meilleure compréhension : « [3] S'il a connaissance d'une vulnérabilité qui représente une cybermenace aiguë pour certaines infrastructures critiques, il en informe immédiatement leurs exploitants, avant même l'élimination ou la divulgation de celle-ci. ».

❖ **Art. 9, al. 4 : réduction ou prolongation du délai**

- *CH++* propose de formuler l'art. 9, al. 4, de façon plus stricte afin de garantir que les délais ne soient pas prolongés dans un trop grand nombre de cas.

- *Swico* suggère de consulter le fabricant avant de raccourcir le délai. Il demande que l'art. 9, al. 4, soit formulé de la manière suivante : « Il [l'OFCS] peut raccourcir le délai après avoir consulté le fabricant lorsque l'élimination de la vulnérabilité ... . ».

- *Le BFC* relève qu'il peut y avoir une contradiction entre « raccourcir le délai si la vulnérabilité peut être facilement exploitée » et « prolonger le délai lorsque l'élimination de la vulnérabilité s'avère particulièrement complexe. ».

❖ **Art. 9, al. 5 : information des exploitants d'infrastructures critiques**

- *CH++* suggère d'affiner la formulation pour ne pas donner l'impression que le DDPS pourrait retenir des informations sur des failles de sécurité dans des situations à risque pour pouvoir éventuellement les utiliser de manière offensive. *CH++* propose de modifier comme suit la formulation potestative de l'art. 9, al. 5 : « Il informe en principe les exploitants d'infrastructures critiques de la présence de vulnérabilités avant même l'élimination ou la divulgation de celles-ci. ».

- Tant *Migros* (information immédiate) que *l'aéroport de ZH* (information obligatoire dans les 72 heures) souhaitent que l'information soit donnée plus rapidement.

- *NEDIK* recommande que l'OFCS informe en principe les exploitants avant l'élimination ou la divulgation de la vulnérabilité, tout en ayant la possibilité d'attendre dans certains cas.

- *Le BFC* se demande comment agir lorsque l'on se trouve en présence d'une vulnérabilité critique et difficile à éliminer. Il suggère de mentionner la possibilité de mettre en place des mesures d'atténuation temporaires jusqu'à l'élimination de la vulnérabilité.

❖ **Art. 9, al. 6 et 7 : coordination avec l'OFCOM**

- *Sunrise* est favorable aux dispositions relatives à la coordination entre l'OFCS et l'OFCOM qu'il considère comme une approche correcte visant à harmoniser et à coordonner les différentes procédures de signalement.

- *La FER* fait remarquer qu'une harmonisation des procédures de l'OFCOM et de l'OFCS pourrait, le cas échéant, s'avérer difficile (p. ex., l'OFCOM doit informer l'OFCS des vulnérabilités afin que celui-ci puisse ensuite, le cas échéant, procéder à leur divulgation coordonnée).

- *Le Parti Pirate Suisse* propose de supprimer l'al. 6 ou de le modifier de sorte que les vulnérabilités puissent continuer à être divulguées conformément aux al. 1 à 4 tout en tenant compte des spécificités propres au contrôle de l'OFCOM. Il estime que le traitement des informations sur les vulnérabilités des infrastructures critiques est imprécis et insuffisant. Aussi, il demande que l'ordonnance règle plus clairement cet aspect.

3.3.2.10 Art. 10 (Soutien aux autorités)

Art. 10 Soutien aux autorités
L'OFCS soutient les autorités de la Confédération et des cantons dans le développement, la mise en œuvre et l'examen de normes et de réglementations dans le domaine de la cybersécurité.

Seuls deux participants à la consultation se sont exprimés sur cette disposition et aucun ne l'a rejetée.

- *UR* s'interroge sur la façon dont les communes seront intégrées dans le processus global.

- *swissuniversities* suggère d'examiner si les hautes écoles ne devraient pas également profiter de ce soutien.

3.3.2.11 Art. 11 (Système de communication permettant l'échange sécurisé d'informations)

Art. 11 Système de communication permettant l'échange sécurisé d'informations
[1] Les autorités et les organisations dont le siège est en Suisse ont accès au système de communication de l'OFCS permettant l'échange sécurisé d'informations (art. 74, al. 2, let. a, LSI).
[2] L'OFCS est responsable de la sécurité du système de communication et de la légalité du traitement des données.

Treize participants à la consultation se sont exprimés sur cette disposition et sur les trois thèmes suivants :

❖ **Accès au système de communication**

- *Le PNR 77/EPFZ/UNIL* relève qu'il n'est pas clair si toutes les autorités et organisations ayant leur siège en Suisse ont accès au système de communication de l'OFCS ou si seules les infrastructures critiques sont concernées. Il recommande de préciser ce point dans l'ordonnance.

- *Swiss Banking*, *Swiss FS-CSC*, *digitalswitzerland*, *economiesuisse* et *scienceindustries* proposent d'étendre l'accès à toutes les organisations et à toutes les autorités soumises à l'obligation de signaler, que leur siège se trouve en Suisse ou non. Ils soutiennent que cela est nécessaire pour renforcer la cyberrésilience sur la place économique suisse et pour faciliter les échanges transfrontaliers pour les entreprises internationales.

❖ **Fonctionnalité et mise en œuvre du système de communication**

- *Swico* accueille favorablement le système de communication central permettant l'échange sécurisé d'informations, mais souligne la nécessité d'avoir des normes de sécurité élevées.

- *BE* exige de clarifier la délimitation entre les systèmes mentionnés aux art. 11 et 12. Il affirme que ni les normes, ni le rapport explicatif ne donnent une explication claire et compréhensible de la délimitation entre les deux systèmes, des différentes utilisations prévues et des objectifs.

- *L'ACS* relève l'importance d'un accès facile sur le plan pratique et d'un enregistrement simple et non bureaucratique pour participer à l'échange d'informations. Elle demande à l'OFCS de veiller à ce que la mise en œuvre de l'ordonnance permette un accès facile.

- *Les CFF* déplorent un manque de clarté concernant les responsabilités en matière de surveillance des nouvelles menaces sur la plateforme de communication de l'OFCS et sur les droits d'accès. Ils souhaitent que ces points soient clarifiés.

❖ **Propositions d'élargissement et de précision**

- *BE* recommande d'introduire, pour les organisations et les autorités assujetties à l'obligation de signaler et pour les exploitants d'infrastructures critiques, l'obligation de s'enregistrer dans le système de communication permettant l'échange sécurisé d'informations ou dans les systèmes d'information permettant l'échange automatique.

- *L'ASA* souligne qu'il est important que l'OFCS établisse un rapport détaillé régulier (anonyme) sur les signalements reçus. La branche des assurances considère que cet aspect est crucial pour contribuer à augmenter la cyberrésilience de l'économie suisse et la pénétration de l'assurance.

- Selon *eAVS/AI*, l'OFCS pourrait exercer une fonction d'interface selon le principe « Once Only » dans le cadre de la mise en œuvre de l'obligation de signaler.

- *Switch* recommande de concrétiser la subsidiarité de l'OFCS dans certains cas et d'ajouter un alinéa supplémentaire qui définisse le principe de la responsabilité individuelle des exploitants privés en matière de cybersécurité.

3.3.2.12 Art. 12 (Systèmes d'information permettant l'échange automatique)

Art. 12 Systèmes d'information permettant l'échange automatique
[1] L'OFCS met à la disposition des exploitants d'infrastructures critiques des systèmes d'information permettant l'échange automatique d'informations techniques sur les cybermenaces et les cyberincidents.
[2] L'OFCS est responsable de la sécurité des systèmes d'information et de la légalité du traitement des données.

Cinq participants à la consultation se sont exprimés sur cette disposition. Ils demandent que le texte de l'ordonnance soit plus clair et plus précis. Leurs propositions concernent également les normes de sécurité, la protection des données et l'accès au système d'information et son utilisation.

❖ **Clarté et précision du texte de l'ordonnance**

- *GL* relève que le texte de l'ordonnance et les commentaires présentent une incohérence au niveau de la terminologie. Alors que le texte de l'ordonnance ne parle que d'« informations techniques », le rapport explicatif mentionne aussi le traitement de données personnelles.

- *SH* fait remarquer que le déroulement de l'échange d'informations entre toutes les parties concernées n'est pas clair. Il demande des règles plus précises sur la manière d'échanger les signalements et les notifications.

❖ **Normes de sécurité et protection des données**

- *L'aéroport de ZH* souhaite que l'OFCS cherche à atteindre les normes de sécurité les plus élevées. Il recommande d'ancrer explicitement cet aspect dans le texte de l'ordonnance.

- *Les CFF* demandent des précisions sur la façon dont les informations peuvent être traitées dans les environnements Cloud. Ils aimeraient en particulier savoir quelles sont les conditions de stockage des informations dans des environnements Cloud en dehors de la Suisse.

❖ **Accès et utilisation du système d'information**

- *swissuniversities* observe que les hautes écoles profiteraient grandement de l'obtention d'informations sur les menaces actuelles (*Threat Intelligence*) directement auprès de l'OFCS ou de *Switch*. Elle souligne ainsi l'importance de l'échange d'informations pour le secteur des hautes écoles.

3.3.2.13 Art. 13 (Enregistrement)

Art. 13 Enregistrement

[1] Les organisations et les autorités sont tenues de s'enregistrer avant de pouvoir utiliser le système de communication. Elles communiquent sans délai toute modification de leurs données.

[2] L'enregistrement doit au moins comporter les informations suivantes:

a. raison sociale, nom ou désignation et adresse de l'organisation ou de l'autorité;

b. les coordonnées de la personne ayant procédé à l'enregistrement.

Huit participants à la consultation se sont exprimés sur cet article et aucun ne l'a rejeté.

❖ **Art. 13, al. 1 : définition et processus d'enregistrement**

- *GE* recommande de remplacer le terme « enregistrement » par « enrôlement » dans la version française de l'art. 13, al. 1, pour éviter toute ambiguïté. Cette modification a pour but de décrire plus précisément le processus d'enregistrement.

- *L'aéroport de ZH* demande un enregistrement obligatoire pour les infrastructures critiques dans les 90 jours suivant l'entrée en vigueur de la loi. Il souligne cependant que la participation à l'échange d'informations doit rester volontaire.

- *swissuniversities* explique que les hautes écoles ont un intérêt à s'enregistrer le plus tôt possible et qu'elles se tiennent à disposition pour tout éventuel pré-enregistrement. Elle propose aussi d'envisager une éventuelle coordination par le biais de *Switch*.

❖ **Art. 13, al. 2 : informations relatives à l'enregistrement et aux coordonnées**

- *GE* suggère d'ajouter une let. c à l'art. 13, al. 2, de la version française pour préciser « les coordonnées de l'unité chargée de la cybersécurité au sein de l'organisation ou de l'autorité ».

- *SH* conseille de ne pas adresser les notifications à une seule personne en cas de signalements critiques, mais de permettre l'enregistrement de plusieurs personnes en vue d'assurer la continuité de la chaîne d'information. *L'aéroport de ZH, digitalswitzerland* et *Swico* s'expriment également en ce sens, puisqu'ils proposent d'utiliser à l'art. 13, al. 2, let. b, les termes « coordonnées d'une ou de plusieurs personnes de contact » au lieu de « coordonnées de la personne ayant procédé à l'enregistrement. ».

- *economiesuisse* et *scienceindustries* demandent la suppression de l'art. 13, al. 2, ou du moins une adaptation de l'art. 13, al. 2, let. b. En effet, elles considèrent que les indications demandées sont trop détaillées et formalistes.

3.3.2.14 Art. 14 (Fournisseurs de prestations)

Art. 14 Fournisseurs de prestations
[1] Les exploitants d'infrastructures critiques peuvent annoncer à l'OFCS des fournisseurs de prestations souhaitant participer à l'échange d'informations.
[2] Les fournisseurs de prestations doivent s'enregistrer en indiquant leur raison sociale ou leur propre nom ainsi que les coordonnées de la personne ayant procédé à l'enregistrement.

Six participants à la consultation se sont exprimés et leurs prises de position montrent qu'ils approuvent cet article. Ils souhaitent toutefois des précisions et formulent des recommandations pour le compléter.

❖ **Art. 14, al. 1 : définition et périmètre des fournisseurs de prestations**

- *FR* recommande d'utiliser les termes « fournisseurs de prestations de cybersécurité » afin d'éviter toute confusion. Cette proposition a pour but de définir plus clairement de quels fournisseurs de prestations il s'agit.

- *GE* propose de préciser dans le texte de l'ordonnance que l'OFCS procède à une analyse des fournisseurs. Cette proposition tient compte du caractère sensible des données à échanger et vise à renforcer la sécurité de l'échange d'informations.

- *VS* demande de préciser si l'article fait référence à tous les fournisseurs de prestations informatiques ou seulement à ceux du domaine de la cybersécurité.

- *Swiss Banking* et *Swiss FS-CSC* proposent de préciser l'article dans le sens que les exploitants d'infrastructures critiques peuvent annoncer à l'OFCS des fournisseurs de prestations leur fournissant des prestations dans le cadre de leurs activités et souhaitant par conséquent participer à l'échange d'informations. L'art. 14, al. 1, serait formulé comme suit : « Les exploitants d'infrastructures critiques peuvent annoncer à l'OFCS les fournisseurs de prestations leur fournissant des prestations dans le cadre de leurs activités (p. ex. dans le cadre d'une externalisation) et souhaitant par conséquent participer avec eux à l'échange d'informations. ». Leur proposition se fonde sur la pratique existante selon laquelle ces fournisseurs de prestations sont déjà autorisés à participer à l'échange d'informations s'ils remplissent les exigences de l'OFCS.

- *Swico* est favorable au fait que les fournisseurs de prestations des exploitants d'infrastructures critiques puissent avoir accès, sur une base volontaire, aux systèmes d'information mentionnés. L'association estime qu'il est judicieux de prévoir une annonce par les exploitants qui débouche sur l'enregistrement du fournisseur de prestations.

❖ **Art. 14, al. 2 : enregistrement des fournisseurs de prestations**

- *Swico* propose de remplacer, à l'art. 14, al. 2, les termes « coordonnées de la personne ayant procédé à l'enregistrement » par « coordonnées d'une ou de plusieurs personnes de contact » : « [2] Les fournisseurs de prestations doivent s'enregistrer en indiquant leur raison sociale ou leur nom ~~ainsi que~~ et ~~les coordonnées de la personne ayant procédé à l'enregistrement~~ les coordonnées d'une ou de plusieurs personnes de contact ». Selon l'association, la formulation actuelle pourrait impliquer une responsabilité de la personne ayant procédé à l'enregistrement, ce qu'il faut éviter.

3.3.2.15 Art. 15 (Transmission et utilisation des informations)

Art. 15 Transmission et utilisation des informations
[1] Les entreprises et les autorités enregistrées transmettent des informations à l'OFCS en indiquant si et à qui elles peuvent être retransmises, dans la mesure où la loi ne prévoit pas un tel processus.
[2] L'OFCS décide de la publication des informations destinées à être transmises sur le système de communication et sur les systèmes d'information en vue de l'échange automatique.
[3] Les destinataires doivent garantir la protection des informations qu'ils reçoivent.
[4] Les fournisseurs de prestations des exploitants d'infrastructures critiques peuvent utiliser les informations qu'ils reçoivent exclusivement à des fins de protection desdites infrastructures.

Au total, douze participants à la consultation se sont penchés sur la disposition relative à la transmission et à l'utilisation des informations. Aucun ne l'a rejetée. Les prises de position contiennent globalement des propositions de précision, d'extension ou d'adaptation de l'article.

❖ **Observations générales sur l'art. 15**

- *SH* s'attend à ce qu'une équipe de soutien spécialisée effectue non seulement un filtrage, mais aussi une catégorisation des signalements. Il est proposé de mettre en place une autorité fédérale centrale disposant d'une expertise claire et jouant un rôle de conseil au niveau national.

- *Swissgrid* se demande quelles seront les conséquences en cas de non-respect de la classification TLP et quelle sera la procédure à suivre si le fournisseur d'informations ne définit pas le cercle des destinataires. Elle souhaite des compléments à ce propos dans l'ordonnance ou dans le rapport explicatif.

- *Le PNR 77/EPFZ/UNIL* propose de préciser la disposition dans le sens que les entreprises et les autorités doivent indiquer, lors de la transmission d'informations, si celles-ci peuvent être transmises et à quelles catégories de destinataires conformément au protocole TLP. Il relève un possible conflit entre les al. 1 et 2 de l'art. 15 et recommande que cet aspect soit clarifié dans l'ordonnance. Le PNR 77/EPFZ/UNIL estime qu'il convient par ailleurs de préciser que l'OFCS ne peut publier des informations que lorsque cela est nécessaire à la protection des infrastructures critiques ou de la Suisse contre les cybermenaces.

❖ **Art. 15, al. 1 : transmission des informations**

- *L'aéroport de ZH* suggère que les entreprises et les autorités enregistrées déterminent quelles informations peuvent être transmises et à qui.

- *GR* recommande qu'il soit possible, lors de la transmission, de déterminer quelles informations peuvent être transmises. En effet, certaines d'entre elles doivent être partagées rapidement alors que d'autres le sont ultérieurement pour des raisons tactiques.

- *NEDIK* indique que la personne ayant procédé au signalement peut gérer elle-même le signalement et que différentes classifications sont possibles. Il insiste sur l'importance d'une classification correcte et relève que les personnes ayant procédé au signalement devraient pouvoir limiter ou exclure la transmission d'informations relatives à certaines données.

- *Swico* souligne combien il est important que l'organisation ou l'autorité transmettant l'information détermine si et à qui les informations peuvent être transmises, en tenant compte de la sensibilité des informations et de la relation de confiance nécessaire.

❖ **Art. 15, al. 2 : publication et transmission des informations**

- *Le MPC* propose de mentionner explicitement que l'OFCS sauvegarde les informations en vue de leur transmission aux autorités de poursuite pénale.

- *Swiss Banking* et *Swiss FS-CSC* demandent de concrétiser les modalités de la transmission des signalements à l'OFCS. Si des signalements groupés sont adressés à différentes autorités, chacune d'entre elles ne devrait pouvoir lire que la partie qui lui est destinée. Ils proposent à cet effet de rajouter deux alinéas à l'art. 15. Le premier serait formulé comme suit : « ^{1bis} Le système mis à disposition par l'OFCS pour la transmission des signalements doit être conçu de sorte que les autorités connectées au système ne puissent lire et traiter que les contenus que l'organisation ayant procédé au signalement leur a destinés. ». Le deuxième alinéa proposé aurait la teneur suivante : « ^{1ter} S'agissant des contenus des signalements partagés par ce biais, l'OFCS décide de la publication ... [suite de l'art. 15, al. 2]. ».

- *La CMP* suggère de limiter la compétence de l'OFCS en matière de transmission d'informations pour garantir une transmission complète des informations aux autorités de poursuite pénale.

- *ZH* recommande que l'OFCS soit tenu de transmettre les signalements de cyberattaques aux autorités de poursuite pénale compétentes en vue d'une évaluation sous l'angle pénal. L'ordonnance devrait ainsi préciser la manière de traiter les informations relevant du droit pénal.

❖ **Art. 15, al. 3 et 4 : protection et utilisation des informations**

- *VS* trouve l'art. 15, al. 4, trop restrictif et propose que les fournisseurs de prestations puissent utiliser les informations sur les vulnérabilités pour mieux protéger les autres clients.

- *NEDIK* rappelle que les autorités de poursuite pénale sont légalement tenues d'ouvrir des enquêtes lorsqu'elles ont connaissance de délits poursuivis d'office. Il demande que l'OFCS s'assure que les informations publiées ne permettent pas d'identifier l'exploitant d'infrastructure critique concerné.

- *Swico* accueille favorablement l'obligation de protéger les informations devant être observée par les destinataires et leur utilisation exclusive pour la protection des infrastructures critiques afin d'éviter les avantages d'une concurrence déloyale.

3.3.2.16 Art. 16 (Exceptions à l'obligation de signaler)

Art. 16 Exceptions à l'obligation de signaler

[1] Les autorités et les organisations ci-après sont exemptées de l'obligation de signaler lorsqu'elles remplissent les conditions suivantes:

a. les organes visés à l'art. 74*b*, al. 1, let. b et c, LSI sont responsables de moins de 1000 habitants; la population résidente est déterminante;
b. les entreprises visées à l'art. 74*b*, al. 1, let. d, LSI, pour autant qu'elles:
    1. ne soient pas tenues, en tant que gestionnaires de réseau, producteurs d'électricité, exploitants de stockage d'électricité ou prestataires visé à l'art. 5*a*, al. 1, et l'annexe 1*a* de l'ordonnance du 14 mars 2008 sur l'approvisionnement en électricité, de respecter le niveau de protection A ou B,
    2. attestent, en tant qu'exploitants de gazoducs visés à l'art. 2, al. 3, de l'ordonnance du 4 juin 2021 sur la sécurité des installations de transport par conduites, un transport annuel d'énergie de moins de 400 GWh en moyenne sur les cinq dernières années;
c. les entreprises visées à l'art. 74*b*, al. 1, let. n, LSI, pour autant qu'elles:
    1. ne soient pas tenues d'installer un système de management de la sécurité de l'information visé aux art. 2 et 4 et à l'annexe II du règlement d'exécution (UE) 2023/203 ou à l'art. 2 et à l'annexe II du règlement délégué (UE) 2022/1645,
    2. ne soient pas tenues d'appliquer les conditions du point 1.7 de l'annexe du règlement d'exécution (UE) 2015/1998 dans leur programme de sûreté visé aux art. 2, 12, 13 ou 14 du règlement (CE) 300/2008;
d. les entreprises ferroviaires, les entreprises d'installations à câbles, de trolleybus, d'autobus et de navigation visées à l'art. 74*b*, al. 1, let. m, LSI, pour autant qu'elles:
    1. ne soient pas chargées de tâches systémiques (art. 37 de la loi fédérale du 20 décembre 1957 sur les chemins de fer [LCdF]),
    2. disposent d'une concession de transport de voyageurs visée à l'art. 6 de la loi du 20 mars 2009 sur le transport de voyageurs (LTV), mais ne fournissent pas de prestations commandées en commun par la Confédération et les cantons (art. 28 à 31*c* LTV),
    3. disposent d'une concession d'infrastructure visée à l'art. 5 LCdF, mais qui n'a pas été octroyée en raison d'un intérêt public à la construction et à l'exploitation de l'infrastructure (art. 6, al. 1, let. a, LCdF);
e. les fournisseurs et les exploitants visés à l'art. 74*b*, al. 1, let. t, LSI dont le siège est en Suisse et qui ne fournissent pas de prestations, en tout ou en partie, à des tiers et contre rémunération.

[2] Les entreprises visées à l'art. 74*b*, al. 1, let. f, g, h, l et p, LSI pour lesquelles l'al. 1 ne s'applique pas sont dispensées de l'obligation de signaler, pour autant qu'elles emploient moins de 50 personnes dans le domaine concerné et que leur chiffre d'affaires annuel ou la somme inscrite au bilan annuel ne dépasse pas 10 millions de francs dans le domaine concerné.

Au total, 24 participants à la consultation se sont exprimés sur cette disposition et aucun ne l'a rejetée. Certains ont toutefois émis des critiques et proposé des modifications ou des compléments.

❖ **Art. 16, al. 1 : exceptions générales à l'obligation de signaler**

– *AG, SZ, VD* et *SwissICT* désapprouvent l'*exception pour les communes* de moins de 1000 habitants, ces dernières pouvant être plus vulnérables aux cyberattaques en raison de leurs ressources réduites. Comme ces communes sont reliées au réseau cantonal, les cyberattaques pourraient avoir des répercussions négatives sur l'infrastructure cantonale. Ces petites communes, souvent les plus vulnérables, sont importantes pour la détection précoce des cyberattaques et les exempter donnerait un mauvais signal. *L'ACS* est favorable à l'exception pour les communes de moins de 1000 habitants. Elle souligne cependant l'importance que revêtent les signalements volontaires et le soutien technique envers toutes les communes.

- En ce qui concerne les *exceptions pour les hautes écoles et les autres institutions, Switch* propose d'exempter dans certains cas les hautes écoles et les registraires de l'obligation de signaler. Il serait en effet disproportionné de soumettre systématiquement ces catégories à l'obligation de signaler. *swissuniversities* recommande d'introduire pour les hautes écoles des valeurs seuils basées sur différents critères tels que la taille, l'infrastructure et les systèmes de recherche.

- *Swiss Banking* et *Swiss FS-CSC* suggèrent de dispenser les organisations et les autorités de l'obligation de signaler les cyberattaques lorsque ces dernières n'ont qu'un impact mineur sur les activités des établissements financiers. Cette exception pourrait être formulée comme suit dans l'al. 1, let. d^{bis} : « d^{bis} les entreprises visées à l'art. 74*b*, al. 1, let. e, LSI, pour autant que les cyberattaques n'aient qu'un impact mineur sur l'activité de l'entreprise et qu'il ne s'agisse pas, en particulier, d'attaques réussies ou partiellement réussies contre des fonctions critiques dont la défaillance ou la perturbation affecterait fortement la protection des clients ou le fonctionnement des marchés. ». Cette disposition peut être concrétisée par une ordonnance de la FINMA ou par une autoréglementation des associations compétentes.

- *Les CFF* sont d'avis qu'ils faudrait reconsidérer les exceptions prévues pour les petits chemins de fer, les exploitants de gazoducs et les entreprises d'électricité, étant donné que ceux-ci peuvent également être touchés par des attaques en rapport avec la sécurité.

- *CH++* et *H+* estiment que les hôpitaux devraient être soumis à l'obligation de signaler, quelle que soit leur taille.

- *L'ASIP* demande un élargissement des exceptions à l'obligation de signaler pour toutes les institutions de prévoyance enregistrées et non enregistrées (avec ou sans prestations réglementaires) gérant jusqu'à 30 000 assurés. Elle estime que la responsabilité de la cybersécurité devrait incomber à l'organe suprême de l'institution de prévoyance et ne pas être inutilement limitée par des dispositions légales.

- *Swissgrid* souhaite que les fournisseurs de prestations gérant des systèmes de mesure et de commande intelligents soient aussi concernés, pour autant qu'ils remplissent certaines valeurs limites.

❖ **Art. 16, al. 2 : exceptions pour les petites structures**

- *Le BFC* s'interroge sur la pertinence de la notion de « petites structures » comme critère d'exception à l'obligation de signaler et pense qu'il serait indiqué de prendre en compte d'autres éléments comme la taille de la clientèle concernée.

- *economiesuisse, scienceindustries* et *Swico* suggèrent que les entreprises et autres organisations de droit privé employant moins de 250 collaborateurs soient exemptées de l'obligation de signaler. Elles proposent de modifier l'art. 16, al. 2, comme suit : « [2] Les entreprises visées à l'art. 74*b*, al. 1, let. f, g, h, l et p, LSI~~, auxquelles l'al. 1 n'est pas applicable,~~ sont exemptées de l'obligation de signaler pour autant qu'elles ~~emploient moins de 50 personnes dans le domaine concerné et si leur chiffre d'affaires annuel ou le total de leur bilan annuel dans le domaine concerné n'excède pas 10 millions de francs~~ emploient moins de 250 collaborateurs au 1er janvier de chaque année. ».

- *SwissICT* recommande de supprimer les exceptions basées sur le nombre de collaborateurs et le chiffre d'affaires d'une entreprise. En effet, elles pourraient compromettre le sens et l'objectif de l'obligation de signaler.

❖ **Autres propositions et observations**

- *L'UVS* demande s'il est prévu de compléter les « Conditions générales pour les prestations TIC ». Elle relève que le rapport explicatif est difficile à comprendre en ce qui concerne cet article.

- *BE* propose de préciser la phrase introductive afin de distinguer les exploitants d'infrastructures critiques des autorités et des organisations : « Les autorités, organisations et exploitants d'infrastructures critiques suivants sont exemptés de l'obligation de signaler aux conditions ci-après : ... . ».

- *GE* fait remarquer qu'il n'est pas clair à l'art. 16, al. 1, let. b, si les deux conditions sont cumulatives ou alternatives.

- *GR* recommande de tenir compte, lors de la définition de la taille des institutions, du risque d'effets en cascade d'un incident lié aux données.

- *SO* trouve que les exceptions à l'obligation de signaler prévues sont cohérentes et compréhensibles.

- *VS* propose d'inverser l'ordre des let. c et d de l'art. 16, al. 1, pour qu'il corresponde à celui de la LSI.

- *Swiss Banking* et *Swiss FS-CSC* conseillent d'éviter les renvois directs à la législation de l'UE (cf. art. 16, al. 1, let. c, ch. 1 et 2, P-OCyS). Comme celle-ci est souvent adaptée, les renvois ne sont pas pertinents, ce qui entraîne un flou juridique.

- *CH++* déplore l'absence de réglementation sur la gestion des risques cumulés.

3.3.2.17 Art. 17 (Obligation de documenter en cas de demande de renseignements sur l'assujettissement à l'obligation de signaler)

Art. 17 Obligation de documenter en cas de demande de renseignements sur l'assujettissement à l'obligation de signaler Les autorités et les organisations intéressées sont tenues de mettre à la disposition de l'OFCS tout document dont il a besoin pour fournir des renseignements sur l'assujettissement à l'obligation de signaler.

Un participant s'est exprimé sur cette disposition et sur la formulation de l'art. 17 qu'il juge imprécise.

- *Le PNR 77/EPFZ/UNIL* désapprouve la formulation peu claire du titre de l'art. 17, du moins dans la version française. Il propose d'utiliser des formulations alternatives telles que « Obligation de mettre à disposition des informations », « Obligation de collaborer » ou « Obligation d'information ».

3.3.2.18 Art. 18 (Cyberattaques à signaler)

Art. 18 Cyberattaques à signaler [1] Le fonctionnement d'une infrastructure critique est mis en péril lorsque: a. des collaborateurs ou des tiers sont touchés par des interruptions de système, ou b. l'organisation ou l'autorité touchée ne peut maintenir ses activités qu'à l'aide de plans d'urgence. [2] Une manipulation ou une fuite d'informations est avérée lorsque: a. des informations importantes pour les affaires sont modifiées ou publiées par des personnes non autorisées;

b. une violation de la sécurité de données est signalée conformément à l'art. 24 de la loi fédérale du 25 septembre 2020 sur la protection des données.

[3] Une cyberattaque est considérée comme étant indétectée pendant une période prolongée si elle s'est produite plus de 90 jours auparavant.

[4] Une cyberattaque est considérée comme étant liée à d'actes de chantage, de menace ou de contrainte lorsque de tels agissements sont dirigés contre une autorité ou une organisation assujettie à l'obligation de signaler, leurs responsables ou leurs collaborateurs, en poste ou anciens, ou contre des personnes agissant pour elle.

33 participants à la consultation ont donné leur avis sur les cyberattaques à signaler. Aucun d'entre eux n'a rejeté l'art. 18 et les opinions exprimées contiennent pour la plupart des propositions de précision, d'extension ou d'adaptation de l'article.

❖ **Art. 18, al. 1 : définition des cyberattaques à signaler**

- De nombreux participants à la consultation ont demandé *des précisions relatives à l'obligation de signaler* :

  - *L'asut* et *Salt* proposent de limiter l'obligation de signaler aux incidents qui ont un impact direct sur le fonctionnement de l'infrastructure critique.

  - *L'aéroport de ZH* demande que seules les cyberattaques réussies ayant des répercussions fonctionnelles soient signalées.

  - *economiesuisse* et *scienceindustries* relèvent qu'il ne faudrait signaler que les attaques réussies entraînant des répercussions fonctionnelles.

  - S'agissant de l'art. 18, al. 1, let. a, *BL* fait remarquer qu'il convient de préciser la notion d'« interruptions de système ». En effet, une interruption du système comptable due à l'utilisation d'une IA n'aura par exemple guère d'impact sur le fonctionnement principal du système.

  - *H+* trouve que la formulation est trop générale et qu'elle devrait être spécifiée.

  - *GR* demande de définir plus précisément le moment auquel une cyberattaque est avérée et de mentionner explicitement les principaux signes d'une attaque sur le point de survenir.

  - *L'ACS* souhaite des précisions concernant la définition des cyberattaques à signaler.

  - *Les CFF* critiquent les formulations qu'ils jugent trop génériques et trop globales et demandent qu'elles soient précisées et limitées.

  - *L'ASA* estime qu'il ne faudrait signaler que les interruptions de système déclenchées intentionnellement.

  - *Swico* propose d'indiquer clairement qu'il doit s'agir d'événements menaçant directement le fonctionnement de l'infrastructure.

  - *SwissICT* suggère de pondérer la définition de la mise en péril du fonctionnement, qu'il considère trop générale.

- *Migros* affirme que toutes les interruptions de système ne mettent pas en péril le fonctionnement d'une infrastructure critique. Aussi, elle propose de ne signaler que les interruptions d'un « système critique pour l'entreprise. ».

- Certains participants à la consultation exigent de *prendre en compte le degré de gravité.* Ainsi*, digitalswitzerland*, *la SUVA* et *la Poste CH SA* suggèrent de tenir compte du degré de gravité d'une cyberattaque à signaler, afin de réduire le travail administratif.

- Les participants à la consultation demandent également la *précision de certains termes* :

  - *NEDIK* affirme que l'ordonnance devrait définir et délimiter plus précisément ce que l'on entend par « défaillance du système ».

  - *GE* propose de préciser dans le rapport explicatif ce qu'il faut comprendre par « part importante ».

  - *GL* recommande d'indiquer plus clairement dans le rapport explicatif que les interruptions de système ne doivent être signalées à l'OFCS que dans le cadre d'une cyberattaque.

❖ **Art. 18, al. 2 : manipulation ou fuite d'informations**

- *Le BFC* fait remarquer qu'il est possible de détecter une fuite d'informations avant que les informations ne soient publiées par des personnes non autorisées.

- *Le PNR 77/EPFZ/UNIL* trouve que le renvoi à la LPD n'est pas idéal. En effet, la LPD prévoit aussi le signalement des violations non intentionnelles de la sécurité des données.

- S'agissant de l'art. 18, al. 1, let. a, *l'ASA* estime que seules les interruptions de système provoquées intentionnellement devraient être signalées et qu'il faudrait ainsi ajouter à l'art. 18, al. 2, qu'il y a manipulation ou fuite d'informations lorsque des informations importantes pour les affaires sont modifiées, publiées et, dans ce cadre, « dérobées, détruites, désactivées ou traitées d'une autre manière par des personnes non autorisées, ce qui a des répercussions à moyen ou long terme sur des applications ou des systèmes essentiels. ». Elle propose par ailleurs de compléter l'art. 18, al. 2, let. c, par une dernière partie de phrase « qui entraîne vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. ».

- *Swiss Banking* et *Swiss FS-CSC* suggèrent de préciser les formulations afin de se concentrer systématiquement sur les cyberattaques et de laisser de côté d'autres aspects comme ceux qui ont trait à la protection des données.

❖ **Art. 18, al. 3 : délai de 90 jours**

- *ZH* pense qu'il serait souhaitable d'avoir une réglementation de base qui indique quels fichiers log peuvent être conservés et pendant combien de temps.

❖ **Art. 18, al. 4 : obligation de signaler en cas d'extorsion, de menace ou de contrainte**

- *BE* propose d'étendre l'obligation de signaler aux anciens responsables et aux anciens collaborateurs d'une autorité ou d'une organisation assujettie à l'obligation de signaler en cas d'extorsion, de menace ou de contrainte ou de renoncer complètement à cette catégorie de personnes.

- *Les CFF* demandent de limiter la portée de l'art. 18, al. 4, afin de ne signaler que les cyberattaques pénalement répréhensibles et crédibles.

❖ **Autres observations relatives à l'art. 18**

- *Le MPC* recommande que l'OFCS signale automatiquement aux autorités de poursuite pénale les cyberattaques susceptibles de constituer des infractions.

- *ISSS* critique le fait que les différents alinéas ne contiennent pas de termes tels que « notamment » ou d'autres formulations similaires qui indiqueraient une énumération non exhaustive.

- *Le Centre* précise que le cercle des destinataires doit être suffisamment large pour que l'obligation de signaler puisse déployer tous ses effets.

- *SH* trouve que la formulation de l'art. 18 est trop courte. Il désapprouve le fait que l'obligation de signaler ne soit pas explicitement mentionnée.

- *UR* estime que les communes ayant une petite population intégrées dans l'un des deux réseaux de centres de calcul ne devraient pas être exemptées de l'obligation de signaler.

- *La CMP* propose d'ajouter un al. 5 qui indiquerait que l'OFCS est tenu de dénoncer au moins les cas visés à l'al. 4 aux autorités de poursuite pénale compétentes.

- *swissuniversities* attire l'attention sur le fait que les hautes écoles doivent se coordonner avec Switch-CERT en cas de signalement à l'OFCS.

3.3.2.19 Art. 19 (Contenu du signalement)

Art. 19 Contenu du signalement

[1] Le signalement d'une cyberattaque contient les informations suivantes:

a. la date et l'heure de la constatation de l'attaque;
b. la date et l'heure de l'attaque;
c. le type d'attaque;
d. les méthodes d'attaque, et
e. les données sur l'agresseur.

[2] Il contient aussi des informations sur l'éventualité d'un chantage, d'une menace ou d'une contrainte en lien avec l'attaque et d'une dénonciation pénale.

[3] Il contient des informations sur les conséquences de la cyberattaque, à savoir:

a. les unités touchées de l'autorité ou de l'organisation;
b. la gravité du préjudice sur la disponibilité, l'intégrité et la confidentialité des informations propres et de celles de tiers, et
c. les effets sur le fonctionnement des unités touchées de l'autorité ou de l'organisation.

[4] Dans le cas où le signalement n'est pas transmis au moyen du système de communication de l'OFCS, il doit aussi contenir des informations sur l'autorité ou l'organisation assujettie à l'obligation de signaler, à savoir:

a. la raison sociale, le nom ou la désignation et l'adresse, et
b. les coordonnées de l'auteur du signalement.

30 participants à la consultation se sont exprimés sur le contenu du signalement et aucun n'a rejeté complètement cette disposition.

❖ **Art. 19, al. 1 : contenu du signalement**

- De nombreux participants à la consultation ont demandé des précisions dans le texte de l'ordonnance concernant l'*étendue et la nature des informations à communiquer* :

  - *BE* et *le PNR 77/EPFZ/UNIL* proposent de remplacer « Angaben zum Verursacher » (données sur l'agresseur) par « Angaben zum Angreifer » (données sur l'attaquant).

  - *GE* recommande de compléter l'art. 19, al. 1, let. e, par « lorsqu'elles sont disponibles ».

  - Afin de tenir compte des attaques visant la chaîne d'approvisionnement et de permettre à l'OFCS d'évaluer correctement la menace nationale*, ZH* suggère d'ajouter l'information suivante au contenu du signalement : « les fournisseurs de prestations ou les autres tiers impliqués. ».

  - *Migros* propose de regrouper les let. c et d qui se rapportent au « type d'attaque » et aux « méthodes d'attaque ».

  - *L'AES* suggère d'ajouter « les systèmes attaqués » à la liste des informations à communiquer.

  - *Le PLR* trouve que la liste des informations est trop longue et difficile à comprendre.

  - *Swiss Banking* et *Swiss FS-CSC* recommandent de compléter l'article afin d'assouplir les exigences relatives au contenu du signalement et de se baser sur les connaissances dont on peut raisonnablement disposer.

  - *La Poste CH SA* et *digitalswitzerland* considèrent qu'il est problématique de donner des informations sur l'agresseur. Elles proposent donc de les demander seulement s'il est possible de les déterminer sans recourir à des procédures forensiques complexes.

  - *NEDIK* relève qu'il n'y a aucune indication quant à la classification à attribuer au signalement en vue de la transmission de l'information et recommande de la définir clairement dès le début.

  - *Primeo* trouve qu'il faudrait également indiquer dans le signalement quel domaine des TO est concerné par l'attaque.

  - *Swissgrid* propose de n'exiger des informations sur l'agresseur que « si elles sont connues » et d'inclure également dans le signalement des informations sur les systèmes attaqués.

- S'agissant des aspects relatifs à la *protection des données et aux données personnelles, l'asut, Salt, Switch* et *Sunrise* font remarquer que le signalement peut aussi comprendre des données personnelles. Ils recommandent de concevoir les procédures de telle sorte que les données personnelles ne soient transmises qu'en cas d'incidents avérés.

❖ **Art. 19, al. 2 : informations supplémentaires**

- *GE* propose une nouvelle formulation pour faciliter la compréhension : « ...des informations sur l'éventualité ou la réalité d'un chantage, ainsi que d'une dénonciation pénale. ».

- *NEDIK* fait observer que le signalement devrait également mentionner l'autorité auprès de laquelle une plainte pénale a été déposée.

- *SwissICT* conseille de supprimer l'art. 19, al. 2, sans le remplacer ou de demander ces informations de manière facultative dans le formulaire de signalement.

❖ **Art. 19, al. 3 : conséquences de la cyberattaque**

- *L'UVS* demande quelle est la différence entre « élevé » et « grave » dans le rapport explicatif et propose des formulations alternatives.

- *L'aéroport de ZH* recommande de mentionner que le signalement doit contenir la fonction des unités touchées.

- *Swiss Banking* et *Swiss FS-CSC* proposent de désigner globalement le degré de gravité de l'attaque par léger, moyen ou grave.

- *economiesuisse* et *scienceindustries* estiment que l'art. 19, al. 3, est trop rigide et va au-delà des dispositions légales. Ils demandent sa suppression.

- *L'AES* précise que l'art. 19, al. 3 se réfère aux « unités touchées de l'autorité ou de l'organisation » et que, par conséquent, les « systèmes attaqués » doivent aussi être ajoutés aux informations mentionnées à l'art. 19, al. 1.

- *Migros* conseille également de supprimer cet alinéa, vu que les informations pertinentes en cas d'urgence dépendent fortement du contexte.

❖ **Art. 19, al. 4 : voie de signalement**

- *L'aéroport de ZH* propose que les organisations soumises à l'obligation de signaler utilisent exclusivement le système de communication de l'OFCS pour émettre leur signalement et que les entreprises non assujetties à l'obligation de signaler puissent aussi signaler une cyberattaque à l'OFCS.

- *GE* recommande d'ajouter un al. 4 à la let. c, dont la formulation serait la suivante : les coordonnées de l'unité chargée de la cybersécurité au sein de l'organisation ou de l'autorité.

❖ **Observations générales sur l'art. 19**

- Pour garantir que seuls les incidents pertinents sont signalés à l'OFCS, *LU* recommande d'introduire des catégories de signalement basées sur les conséquences de l'événement : incident mineur (aucun signalement ou alors optionnel), incident moyen (signalement obligatoire dans la semaine) et incident majeur (signalement obligatoire dans les 24 heures).

- *VS* propose de centraliser les signalements des cyberattaques à l'OFCS afin d'éviter les signalements multiples à différents services fédéraux.

- *La FER* relève que l'évaluation des conséquences des cyberattaques peut être subjective et varier d'une organisation à l'autre.

- Selon *ISSS*, il faudrait faire une distinction entre le contenu du signalement initial et, selon la classification de l'incident, les autres contenus.

- *Les CFF* considèrent que les informations demandées sont en partie illusoires et irréalistes. Ils demandent que l'article soit adapté de sorte qu'un signalement puisse se faire même si toutes les données ne sont pas disponibles.

- *L'ASA* recommande d'harmoniser le seuil d'entrée des signalements entre la LSI et la LPD.

- *L'aéroport de ZH* exige que l'OFCS ne puisse pas transmettre des informations aux autorités de poursuite pénale et à d'autres autorités sans l'accord de l'autorité ou de l'organisation soumise à l'obligation de signaler.

- *Switch* propose de concrétiser la disposition à plusieurs égards, notamment en fixant une limite temporelle et une limite relative au nombre de personnes concernées.

3.3.2.20 Art. 20 (Transmission du signalement)

Art. 20 Transmission du signalement
Dans le cas où le signalement n'est pas transmis au moyen du système de communication de l'OFCS, ce dernier informe la personne de contact visée à l'art. 13, al. 2, let. b, de la réception et du contenu du signalement.

Cinq participants à la consultation se sont exprimés sur la transmission du signalement et aucun n'a rejeté la disposition. Les prises de position contiennent des demandes de compléments et de précision.

❖ **Signalement par l'intermédiaire d'organisations tierces**

- *Switch* propose qu'une ou plusieurs entreprises puissent décider, individuellement ou conjointement, de transmettre leurs signalements par l'intermédiaire d'une organisation tierce spécialisée qui prendrait également en charge la réponse aux incidents.

- *swissuniversities* conseille d'ajouter à l'art. 20 un alinéa mentionnant qu'une ou plusieurs entreprises peuvent décider individuellement ou conjointement de signaler des incidents par le biais d'une organisation tierce spécialisée. Ils proposent une formulation concrète à cet effet : « [2] Une ou plusieurs autorités ou organisations assujetties à l'obligation de signaler peuvent décider d'externaliser, individuellement ou collectivement, le processus de signalement à une organisation tierce spécialisée. ».

❖ **Anonymat des signalements**

- *economiesuisse, scienceindustries* et *digitalswitzerland* proposent d'adapter la formulation afin de garantir l'anonymat des signalements de tiers. Ils recommandent également une formulation n'autorisant la communication des coordonnées que dans les cas où cela est nécessaire pour protéger la cybersécurité : « Dans le cas où un signalement n'est pas transmis au moyen du système de communication de l'OFCS, ce dernier informe la personne de contact visée à l'art. 13, al. 2, let b, d'une organisation enregistrée et concernée par le signalement de la réception et du contenu du signalement, sans toutefois dévoiler les coordonnées de l'organisation ou de la personne ayant effectué le signalement, à moins que ces coordonnées ne soient également nécessaires pour protéger la cybersécurité. ».

3.3.2.21 Art. 21 (Délai de saisie du signalement)

Art. 21 Délai de saisie du signalement
[1] Si toutes les informations nécessaires ne sont pas communiquées dans les 24 heures, l'OFCS accorde à l'autorité ou à l'organisation concernée un délai de 14 jours pour compléter le signalement.
[2] Si les informations nécessaires n'ont pas toutes été fournies dans le délai accordé, l'OFCS demande à l'autorité ou à l'organisation concernée de les compléter immédiatement ou de confirmer que les informations ne sont pas disponibles.

Dix participants à la consultation se sont exprimés sur la disposition relative au délai de saisie du signalement et aucun ne l'a rejetée. Les prises de position contiennent des propositions de compléments et de précision.

❖ **Délai de 24 heures pour le premier signalement**

- *Le PNR 77/EPFZ/UNIL* recommande d'affiner la formulation « dans les 24 heures suivant la découverte de la cyberattaque » afin de faciliter la compréhension pour les autorités et les organisations assujetties à l'obligation de signaler.

- *Switch* estime que le délai de 24 heures entraînera une charge de travail disproportionnée, surtout pour les petites organisations. Il propose que le délai de 24 heures se réfère aux semaines de travail et aux heures de bureau.

- *Swissgrid* suggère de préciser dans l'ordonnance que le signalement doit s'effectuer dans les 24 heures suivant la découverte de la cyberattaque ou d'ajouter un renvoi direct à l'art. 74*e*, al. 1, LSI.

- *swissuniversities* attire l'attention sur le fait que les exigences concernant le délai de signalement de 24 heures représentent des défis importants pour les petites hautes écoles eu égard à la maturité des processus existants et au personnel engagé ou nécessaire.

❖ **Délai de 14 jours pour les signalements ultérieurs**

- *LU* indique de mentionner si le délai de 14 jours pour compléter le signalement concerne les jours ouvrables ou les jours de la semaine.

- *SwissICT* recommande de raccourcir le délai de 14 jours pour les signalements ultérieurs. Il propose par ailleurs de préciser ce que l'OFCS fait des informations recueillies.

❖ **Adaptation des délais aux normes internationales**

- *economiesuisse* et *scienceindustries* souhaitent que l'on aligne les obligations de signaler sur les normes internationales et que l'on adapte en conséquence les délais à ceux de la directive européenne NIS 2 (24 heures pour une alerte précoce, 72 heures pour le signalement d'un incident).

❖ **Rôle de l'OFCS et aide à la collecte d'informations**

- *eAVS/AI* propose de préciser à l'art. 21 que la collecte d'autres informations qui, le cas échéant, ne peuvent pas être recueillies directement s'effectue lors d'un échange et avec le soutien de l'OFCS.

❖ **Sanctions en cas de non-respect**

- *UR* se demande quelles sont les sanctions prévues lorsqu'une autorité concernée ne fournit pas les informations requises et ne respecte pas l'obligation de signaler à l'OFCS.

3.3.2.22 Art. 22

Art. 22 Modification d'autres actes La modification d'autres actes est réglée en annexe.

L'art. 22 n'a fait l'objet d'aucun retour.

3.3.2.23 Art. 23

Art. 23 La présente ordonnance entre en vigueur le 1er janvier 2025.

Dix participants à la consultation se sont prononcés sur l'entrée en vigueur et aucun d'entre eux n'a rejeté l'article. Les prises de position demandent une entrée en vigueur de l'obligation de signaler plus tardive.

❖ **Demande d'une période transitoire d'au moins six mois**

- *L'asut, Salt* et *Sunrise* proposent un délai d'introduction d'au moins six mois afin de donner aux entreprises suffisamment de temps pour adapter leurs processus et leurs systèmes techniques.

❖ **Demande d'une période transitoire d'au moins neuf mois**

- *SUISSEDIGITAL* souhaite un délai transitoire d'au moins neuf mois entre la publication du texte officiel de l'OCyS et le début effectif de l'obligation de signaler.

❖ **Demande d'une période transitoire d'au moins douze mois**

- *Le PLR, Swiss Banking* et *Swiss FS-CSC* proposent une période transitoire d'au moins un an, de préférence de deux ans, entre le moment où le texte final de l'ordonnance sera disponible et son entrée en vigueur.

- *L'ASA, La Poste CH SA, economiesuisse* et *scienceindustries* estiment qu'une entrée en vigueur au 1er janvier 2025 est trop précoce. Ils demandent un délai de mise en œuvre d'au moins un an après la publication officielle de l'ordonnance.

3.3.2.24 Ordonnance du 7 mars 2003 sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports (Org-DDPS)

Art. 15*a*, al. 2, phrase introductive et let. f et h 2 Il assume notamment les tâches suivantes: f. il gère l'équipe nationale d'intervention en cas d'urgence informatique (*Computer Emergency Response Team [CERT]*); h. il représente la Suisse dans les organes internationaux dans le cadre de l'analyse technique des cybermenaces et la maîtrise des cyberincidents.

Trois participants à la consultation se sont exprimés sur les modifications de l'Org-DDPS et aucun ne les a rejetées. Les prises de position contiennent des propositions de précision et d'adaptation.

❖ **Étendue et limitation de la participation internationale de l'OFCS**

- *ZH* suggère de préciser l'étendue de la participation de l'OFCS aux organes internationaux et de la limiter au domaine de la cybersécurité. Il souligne qu'il ne faut pas restreindre les échanges nationaux et internationaux entre les autorités de poursuite pénale pour se protéger préventivement contre les cybermenaces et pour gérer répressivement les cyberincidents.

- *La CMP* demande que l'art. 15*a*, al. 2, let. h, Org-DDPS définisse plus précisément l'étendue des travaux des organes de l'OFCS et qu'ils soient limités au domaine de la cybersécurité. Elle relève également que cette disposition ne doit pas restreindre les échanges nationaux et internationaux des autorités de poursuite pénale effectués pour se protéger préventivement contre les cybermenaces et pour gérer répressivement les cyberincidents.

❖ **Déplacement et uniformisation de la liste des tâches**

- *VS* suggère de transférer la liste des tâches de l'art. 15*a* Org-DDPS dans l'OCyS et de généraliser l'acronyme français OFCS ou sa version anglaise NCSC dans toutes les bases légales existantes (LSI, OPCy et OCyS).

3.3.2.25 Ordonnance du 31 août 2022 sur la protection des données (OPDo)

Art. 41, al. 1 *Abrogé*

Personne ne s'est prononcé sur l'abrogation de l'art. 41, al. 1, OPDo.

3.3.2.26 Autres remarques

Neuf participants à la consultation ont formulé d'autres remarques dans leurs réponses, sans se référer directement au texte de l'ordonnance :

❖ **Coordination centrale effectuée par l'OFCS**

- *L'aéroport de ZH* propose un nouvel article prévoyant qu'un signalement à l'OFCS annule automatiquement toute autre obligation de signaler en cas de cyberattaque. L'OFCS doit fonctionner comme un service de coordination et coordonner les demandes des autorités.

- *La Poste CH SA* suggère que l'OFCS reçoive tous les incidents à signaler et les coordonne ensuite avec d'autres services d'autorités concernées. Elle propose alternativement que les autorités auxquelles il faut s'adresser se coordonnent entre elles.

- *digitalswitzerland* propose que l'OFCS joue un rôle central et coordinateur au niveau des signalements afin d'éviter un surcroît de travail et des doublons.

- *economiesuisse* et *scienceindustries* déplorent le manque de coordination ou d'harmonisation entre les nombreuses procédures de signalement des cyberattaques et demandent des solutions pour les harmoniser et les coordonner.

- *Migros* souligne l'importance d'une approche basée sur la collaboration lors de la mise en œuvre des procédures de signalement harmonisées. Elle propose de se concentrer sur le renforcement d'un dialogue partenarial entre les autorités et les représentants des infrastructures critiques et d'accorder moins d'importance au formalisme.

- *Swico* salue le renforcement du rôle de l'OFCS en tant qu'organisme central et coordinateur, mais estime qu'il est nécessaire d'harmoniser les nombreuses procédures de signalement.

❖ **Autres thèmes**

- *LU* demande une définition plus claire de la notion de « sérieux dommages » en tant qu'élément de la Cyberstratégie nationale dans le contexte de la lutte contre la cybercriminalité.

- *digitalswitzerland* propose d'instaurer des incitations pour un comportement proactif concernant le signalement des cybervulnérabilités et d'établir une liste de critères spécifiques pour prioriser les signalements.

- Les propositions et recommandations de *Beat Lehmann*, qui n'a pas formulé de commentaires spécifiques sur les différents articles et alinéas de l'ordonnance, sont reprises ci-dessous par thème :

    - *Obligations de signaler* : il indique qu'il convient de tenir compte des différentes situations telles que l'apparition en masse de perturbations et l'obligation de signaler lors du traitement des commandes et dans les entreprises affiliées. Il demande en outre d'harmoniser les différentes obligations de signaler d'après les différentes lois et recommande de coordonner les obligations de signaler en cas de cyberattaques transfrontalières. Il propose également que l'OFCS ait la compétence de publier des aide-mémoires ou des directives concernant des groupes de cas typiques.

    - *Menaces dynamiques* : il attire l'attention sur les perturbations possibles de l'infrastructure informatique par des États étrangers ou leurs agents. Il insiste à cet égard sur le danger des cyberattaques en tant qu'élément de la guerre hybride et de la désinformation ciblée et souligne que non seulement le traitement classique des données, mais aussi la technologie opérationnelle (TO) et les systèmes SCADA peuvent être la cible de cyberattaques. Il relève par ailleurs le rôle clé de l'intelligence artificielle dans le développement de moyens et de procédures de cyberattaques et dans la défense contre ces dernières.

    - *Coopération internationale* : il recommande de mettre en évidence les possibilités de collaborations internationales de l'OFCS avec l'OCDE, l'UE / l'ENISA et l'OTAN.

    - *Partenariat public-privé* : il propose que la LSI élargie et l'OCyS constituent la base d'un « partenariat public-privé » global entre les autorités publiques à tous les niveaux, l'économie et la science.

4 Annexe

4.1 Cantons

GT	Staatskanzlei des Kantons AG	Regierungsgebäude 5001 Aarau
AI	Ratskanzlei des Kantons AI	Marktgasse 2 9050 Appenzell
BE	Chancellerie d'État du canton de Berne	Postgasse 68 3000 Berne 8
BL	Landeskanzlei des Kantons Basel-Landschaft	Regierungsgebäude Rathausstrasse 2 4410 Liestal
BS	Staatskanzlei des Kantons Basel-Stadt	Marktplatz 9 4001 Basel
FR	Chancellerie d'État du canton de Fribourg	Rue des Chanoines 17 1701 Fribourg
GE	Chancellerie d'État du canton de Genève	Rue de l'Hôtel-de-Ville 2 Case postale 3964 1211 Genève 3
GL	Staatskanzlei des Kantons GL	Rathaus 8750 Glaris
GR	Standeskanzlei des Kantons GR	Reichsgasse 35 7001 Chur
LU	Staatskanzlei des Kantons LU	Bahnhofstrasse 15 6002 Luzern
NW	Staatskanzlei des Kantons NW	Dorfplatz 2 Postfach 1246 6371 Stans
OW	Staatskanzlei des Kantons OW	Rathaus 6061 Sarnen
SG	Staatskanzlei des Kantons SG	Regierungsgebäude 9001 St. Gallen
SH	Staatskanzlei des Kantons SH	Beckenstube 7 8200 Schaffhausen
SO	Staatskanzlei des Kantons SO	Rathaus Barfüssergasse 24 4509 Solothurn
SZ	Staatskanzlei des Kantons SZ	Regierungsgebäude Bahnhofstrasse 9 6431 Schwyz
TG	Staatskanzlei des Kantons Thurgau	Regierungsgebäude Zürcherstrasse 188 8510 Frauenfeld
TI	Cancelleria dello Stato del Cantone Ticino	Piazza Governo 6 6501 Bellinzona
UR	Standeskanzlei des Kantons Uri	Rathausplatz 1 6460 Altdorf
VD	Chancellerie d'État du canton de Vaud	Place du Château 4 1014 Lausanne

VS	Chancellerie d'État du canton du Valais	Planta 3 1950 Sion
ZG	Staatskanzlei des Kantons Zug	Seestrasse 2 Regierungsgebäude am Postplatz 6300 Zug
ZH	Staatskanzlei des Kantons ZH	Neumühlequai 10 Postfach 8090 Zürich

4.2 Conférences cantonales et commissions fédérales

BFC	Bureau fédéral de la consommation	Bureau fédéral de la consommation (BFC) Palais fédéral Est 3003 Berne
CCDJP	CCDJP Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP)	Maison des cantons Speichergasse 6 Case postale 3001 Berne
CMP	Conférence suisse des ministères publics	Maison des cantons Speichergasse 6 Case postale 3001 Berne

4.3 Partis politiques représentés à l'Assemblée fédérale

Le Centre		Secrétariat général Seilerstrasse 8a Case postale 3001 Berne
PLR	PLR. Les Libéraux-Radicaux	Secrétariat général Neuengasse 20 Case postale 3001 Berne
PS	Parti socialiste suisse PS	Secrétariat central Theaterplatz 4 Case postale 3001 Berne

4.4 Associations faîtières des communes, des villes et des régions de montagne œuvrant au niveau national

ACS	Association des communes suisses (ACS)	Holzikofenweg 8 Case postale 3001 Berne
UVS	Union des villes suisses (UVS)	Monbijoustrasse 8 Case postale 3001 Berne

4.5 Associations faîtières œuvrant au niveau national

economie-suisse	Fédération des entreprises suisses	Hegibachstrasse 47 Case postale 8032 Zurich
USS	Union syndicale suisse	Monbijoustrasse 61 3007 Berne
sgv/usam	Union suisse des arts et métiers	Schwarztorstrasse 26 Case postale 3001 Berne
Swiss Banking	Association suisse des banquiers	Aeschenplatz 7 Postfach 4182 4002 Bâle

4.6 Autres organisations intéressées

ASIP	Association suisse des institutions de prévoyance	Kreuzstrasse 26 8008 Zurich
asut	Association suisse des télécommunications	Hirschengraben 8 3011 Berne
MPC	AS-MPC	Guisanplatz 1 3003 Berne
Beat Lehmann		Acting Counsel RioTinto / Alcan Holdings Switzerland AG Kongoweg 9 (bureau à domicile) 5034 Suhr
digital-switzer-land	digitalswitzerland	Waisenhausplatz 14 3011 Berne
eAVS/AI		c/o mundi consulting ag Marktgasse 55 Case postale 3001 Berne
FAMH	Association des laboratoires médicaux de Suisse (FAMH)	Altenbergstrasse 29 Case postale 686 3000 Berne 8
FER	Fédération des entreprises romandes (FER)	Rue de Saint-Jean 98 1211 Genève
Aéroport de GE		Aéroport international de Genève Case postale 100 1215 Genève
Aéroport de ZH		Aéroport de ZH SA 8058 Zürich Flughafen
H+	H+ Les Hôpitaux de Suisse	Secrétariat central Lorainestrasse 4A 3013 Berne
ISSS	Information Security Society Switzerland	Zentweg 13 3006 Bern
Migros	Migros	Migros Direction politique économique Limmatstrasse 152

		Case postale 1766 8031 Zurich
NEDIK	NEDIK (réseau de soutien aux enquêtes dans la lutte contre la criminalité informatique), rattaché à la CCPCS et à la CCDJP	c/o Secrétariat général CCDJP Maison des cantons Speichergasse 6 Case postale 3001 Berne
PNR 77 EPFZ UNIL	Position commune	
Parti Pirate Suisse	Parti Pirate Suisse	Parti Pirate Berne 3000 Berne
Poste CH SA	Poste CH SA	Wankdorfallee 4 Case postale 3030 Berne
Pour Demain	Pour Demain	Marktgasse 46 3011 Berne
Primeo		Weidenstrasse 27 4142 Münchenstein
RAILplus SA	RAILplus SA	Bahnhofstrasse 85 5001 Aarau
Salt		Salt Mobile SA Rue du Caudray 4 1020 Renens 1
CFF		CFF SA Public Affairs and Regulation Hilfikerstrasse 1 3000 Berne 65
science-industries	Association des industries Chimie Pharma Life Sciences	Nordstrasse 15 Case postale 8021 Zurich
Suissedigital	Association de réseaux de communication	Bollwerk 15 3011 Berne
Sunrise		Sunrise GmbH Thurgauerstrasse 101B 8152 Glattpark (Opfikon)
SUVA		Fluhmattstrasse 1 Case postale 4358 6004 Lucerne
ASA	Association suisse d'assurances	Conrad-Ferdinand-Meyer-Strasse 14 Case postale 8022 Zurich
Swico	Swico	Lagerstrasse 33 8004 Zurich
Swiss FS-CSC	Swiss Financial Sector Cyber Security Centre (Swiss FS-CSC)	Aeschenplatz 7 Case postale 4182 4002 Bâle
Swissgrid		Bleichemattstrasse 31 Postfach 5001 Aarau

Swiss-ICT	SwissICT	Vulkanstr. 120 8048 Zurich
swissuni-versities	Organisation faîtière des hautes écoles suisses	swissuniversities Effingerstrasse 15 Case postale 3001 Berne
Switch		Werdstrasse 2 Case postale 8021 Zurich
Transit-gas	Transitgas AG	Franklinstrasse 27 8050 Zurich
CH++	Organisation CH++	Sattelgasse 4 4051 Bâle
AES	Association des entreprises électriques suisses	Hintere Bahnhofstrasse 10 5000 Aarau