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)

Commentaires concernant l'ordonnance sur la cybersécurité (OCyS)

22 mai 2024

Table des matières

1 Contexte

Le 11 décembre 2020, le Conseil fédéral a chargé le Département fédéral des finances d'élaborer les bases légales nécessaires à l'introduction d'une obligation de signaler les cyberattaques visant les infrastructures critiques. Le Conseil fédéral a alors 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)[1] à l'intention du Parlement. Ce dernier a ensuite approuvé les modifications de la LSI le 29 septembre 2023[2] ; le délai référendaire a expiré le 18 janvier 2024 sans avoir été utilisé.

Le présent projet d'ordonnance 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 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 loi sur la sécurité de l'information 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 contre les infrastructures critiques. L'ordonnance du 27 mai 2020 sur les cyberrisques (OPCy)[3] a également été abrogée à cette date[4]. 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)[5]. 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 Département fédéral de la défense, de la protection de la population et des sports (DDPS) le 1er janvier 2024. Pour cette raison, des dispositions organisationnelles sur l'OFCS figurent à l'art. 15*a*, al. 1 et 2, let. a à g, Org-DDPS[6].

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. La future ordonnance sur la cybersécurité (OCyS) réglera ainsi les tâches de l'OFCS et l'obligation de signaler les cyberattaques contre les infrastructures critiques en complément de l'OSI. Elle porte donc surtout sur les relations entre l'OFCS et les assujettis 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.

1 RS **128**
2 FF **2023** 2296
3 RS **120.73**
4 RO **2023** 735 (annexe 2, ch. I)
5 RS **128.1**
6 RS **172.214.1**

2 Commentaires des dispositions

Section 1 Objet

Art. 1

Cette disposition s'appuie sur les bases légales mentionnées au « Chapitre 5 : Mesures de la Confédération afin de protéger la Suisse contre les cybermenaces » de la loi sur la sécurité de l'information (art. 73*a* ss LSI) et également sur l'art. 15*a,* al. 1 et 2, let. a à g, Org-DDPS.

L'art. 1 décrit l'objet de l'ordonnance et reproduit, aux let. a à d, la structure de l'ordonnance, qui correspond également aux titres des différentes sections :

Let. a *Cyberstratégie nationale et comité de pilotage*

L'ordonnance prévoit aux art. 2 à 5 que la Confédération définit une Cyberstratégie nationale (CSN) en accord avec les cantons et constitue un comité de pilotage (CP CSN) pour sa mise en œuvre. Elle précise sa composition, son organisation et ses tâches.

Let. b *Tâches de l'OFCS*

Aux art. 6 à 10, l'ordonnance définit et complète les tâches de l'OFCS visées à l'art. 73*a*, al. 2, LSI. Jusqu'à fin 2023, les tâches du NCSC, l'organisation qui a précédé l'OFCS, étaient réglées dans l'OPCy, qui a été abrogée. Dans le cadre de la révision de la LSI, ces tâches ont été intégrées dans une loi formelle.

Let. c *Échange d'informations entre l'OFCS et les autorités et organisations chargées de la protection contre les cyberincidents et les cybermenaces*

Aux art. 11 à 15, l'ordonnance règle l'échange d'informations entre l'OFCS et les autorités et organisations chargées de la protection contre les cyberincidents et les cybermenaces concernant les incidents, les menaces et les attaques en cours dans le domaine de la cybersécurité. Elle précise les directives, les compétences et les responsabilités applicables au système de communication permettant l'échange sécurisé d'informations et aux systèmes d'information pour l'échange automatique, le tout afin de garantir une transmission rapide et efficace des informations pertinentes aux bons destinataires.

Let. d *Obligation de signaler les cyberattaques*

Au cours de la procédure de consultation sur la révision de la LSI, il a été plusieurs fois demandé que les dispositions sur l'obligation de signaler les cyberattaques contre les infrastructures critiques soient concrétisées au niveau de l'ordonnance. Les art. 16 à 21 de la présente ordonnance répondent à cette attente, exprimée à plusieurs reprises dans le message relatif à la modification de la loi sur la sécurité de

l'information[7]. L'ordonnance détaille notamment l'obligation de signaler et précise quelles autorités et organisations en sont exemptées, quelles cyberattaques doivent être signalées, mais aussi quels sont le contenu, le volume des signalements et le déroulement de la procédure afférente.

Il mérite d'être mentionné dans le cadre de l'énumération exhaustive de l'objet de réglementation qui figure dans cet article que toutes les directives en matière de cybersécurité de l'administration fédérale, les compétences et les tâches du service spécialisé de la Confédération pour la sécurité de l'information et les interfaces qui en résultent avec les tâches de l'OFCS sont réglées dans l'OSI.

Les mesures de cyberdéfense ne sont pas régies par l'ordonnance sur la cybersécurité. Celles-ci se rapportent aux mesures militaires et de renseignement et incluent notamment les mesures actives prévues à l'art. 37 de la loi fédérale du 25 septembre 2015 sur le renseignement[8] afin de perturber et de ralentir les cyberattaques. Elles concernent aussi les mesures de l'armée visant à garantir sa disponibilité opérationnelle dans toutes les situations et à mettre à disposition des capacités destinées à appuyer subsidiairement les autorités civiles. Ces mesures sont réglées dans la loi sur le renseignement, la loi sur l'armée[9] et les ordonnances correspondantes.

Section 2 Cyberstratégie nationale et comité de pilotage

Art. 2 Cyberstratégie nationale

Jusqu'à fin 2023, les dispositions relatives à la cyberstratégie nationale figuraient à l'art. 5 de l'OPCy abrogée. Selon cet article, qui s'inscrit dans la continuité de la réglementation précédente, le Conseil fédéral est tenu de fixer dans la CSN les objectifs et les mesures dans le domaine de la protection face aux cyberrisques. Conformément à l'art. 15*a*, al. 2, let. g, Org-DDPS, l'OFCS est chargé au sein de l'administration fédérale d'élaborer la CSN à l'intention du Conseil fédéral et de coordonner sa mise en œuvre.

La CSN fixe, conformément à l'*al. 1*, le cadre stratégique de la prévention dans le domaine de la cybersécurité, de la détection précoce des cybermenaces, des possibilités de réaction et de la résilience en cas d'incident afin de protéger le pays des cyberincidents et des cybermenaces. Ceci signifie que la CSN suit une approche globale pour gérer les cyberincidents et les cybermenaces qui englobe plusieurs aspects de la cybersécurité :

- *Prévention dans le domaine de la cybersécurité* : la prévention se rapporte aux mesures prises pour identifier de possibles vulnérabilités et méthodes d'attaque et les réduire à un minimum. À cet effet, des directives de sécurité

7 Message du 2 décembre 2022 relatif à la modification de la loi sur la sécurité de l'information (mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), FF **2023** 84

8 RS **121**

9 Loi fédérale sur l'armée et l'administration militaire (LAAM ; RS 510.10).

peuvent être mises en place, des formations organisées pour le personnel, des audits de sécurité effectués et des technologies de sécurité utilisées.

- *Détection précoce des cybermenaces* : la détection précoce des cybermenaces est l’aptitude à détecter précocement des signes de cyberincidents et de cybermenaces. Elle inclut la surveillance des activités suspectes sur les réseaux et les systèmes et la mise en place de technologies pour identifier incidents et menaces.

- *Possibilités de réaction en cas d’incident :* les possibilités de réaction en cas d’incident représentent la capacité à réagir de manière appropriée à des cyberincidents et des cybermenaces dès leur identification. Elles peuvent impliquer l’activation de l’équipe d’intervention en cas d’urgence informatique (*Computer Emergency Response Team* [CERT]), l’engagement de contre-mesures et la collaboration avec d’autres autorités ou organisations visant à gérer l’incident ou la menace.

- *Résilience en cas d’incident* : la résilience se rapporte notamment à la vitesse de rétablissement d’un système après une cyberattaque. Elle implique par exemple la mise en place de systèmes de sauvegarde, de plans d’urgence et d’autres mesures visant à réduire au maximum les conséquences d’une attaque.

- *Lutter efficacement contre la cybercriminalité et la poursuivre* : l'infrastructure numérique disponible sur Internet offre aux délinquants potentiels de nouvelles possibilités, avec un potentiel de dommages importants pour la société et l'économie. La cybercriminalité franchit les frontières territoriales, et ce dans le cadre d'un processus hautement dynamique avec des cycles d'innovation courts. Plus l'interconnexion numérique est développée, plus le risque est grand que les cyberincidents commencent certes dans le monde virtuel, mais qu'ils déploient leurs effets dommageables dans le monde réel. Dans le contexte de cette évolution, il est important de continuer à améliorer l'interopérabilité et la capacité de réaction à l'échelle nationale et en collaboration avec des partenaires internationaux, ainsi que d'harmoniser efficacement les compétences professionnelles, techniques et personnelles, sans pour autant déplacer les compétences entre les différentes autorités et les différents niveaux de l'État.

La CSN fixe le cadre de ces différents aspects et coordonne les efforts au niveau national conformément à l’*al. 2*, en accord avec les cantons. Une stratégie globale vise à s’assurer que la Suisse dans son ensemble soit mieux protégée des cyberincidents et des cybermenaces et qu’elle puisse y réagir efficacement.

Art. 3 Instauration et organisation du CP CSN

Jusqu’à fin 2023, les fonctions et la composition du comité de pilotage de la Cyberstratégie nationale (CP CSN) étaient réglées à l’art. 9 de l’OPCy abrogée.

Al. 1 : Instauration du CP CSN par le Conseil fédéral

L'*al. 1* prévoit que le CP CSN est instauré par le Conseil fédéral afin de conférer à ce comité le poids politique nécessaire. Celui-ci pilote et surveille la mise en œuvre de la CSN et coordonne les mesures de renforcement de la cybersécurité au niveau national. Le CP CSN joue un rôle important dans l'élaboration d'une approche globale de gestion des cyberincidents et des cybermenaces en Suisse. En coordonnant et en surveillant les mesures de mise en œuvre de la CSN, il contribue à améliorer la protection de la Suisse contre les cyberincidents et les cybermenaces et concourt à l'efficacité de la réaction du pays face aux dangers actuels.

Al. 2 : Organisation du CP CSN

L'OFCS met à disposition le secrétariat du CP CSN conformément à l'*al. 2.* Il a par conséquent une fonction de soutien administratif et organisationnel vis-à-vis du comité et aide à coordonner les activités de ce dernier, à préparer les séances, à rédiger les procès-verbaux et les rapports et à assurer la communication avec les membres et autres acteurs concernés. En mettant le secrétariat à disposition, l'OFCS permet au CP CSN de travailler efficacement et soutient un peu plus la mise en œuvre de la CSN. Il apporte ce faisant ses connaissances techniques dans le domaine de la cybersécurité et soutient une collaboration efficace entre les différents membres du comité.

Art. 4 Composition du CP CSN

Al. 1 : Membres du CP CSN

Concernant la composition du CP CSN, il faut noter que la CSN est une stratégie nationale qui ne se limite pas aux seules activités de la Confédération. Il est donc important que les cantons, l'économie, la société et les hautes écoles y soient représentés. La mise en œuvre de la CSN exige une participation large et variée et la composition du CP CSN reflète cette nécessité.

- Les *représentants des départements et de la Chancellerie fédérale* se font l'écho de l'administration fédérale et sont responsables de la coordination et de la mise en œuvre de mesures au niveau fédéral.

- Les *représentants des cantons* garantissent la prise en compte des intérêts et des besoins des cantons en matière de cybersécurité. De nombreux aspects de la cybersécurité concernent les cantons, d'où la nécessité de les y associer afin que la stratégie nationale soit efficace.

- Les *représentants de l'économie, de la société et des hautes écoles* relaient différents points de vue et connaissances techniques. Cible souvent privilégiée des cyberincidents et des cybermenaces, l'économie peut apporter de précieuses informations sur ces sujets. La société représente les intérêts des citoyennes et des citoyens eu égard à la sécurité numérique et au fonctionnement des infrastructures critiques. Les hautes écoles peuvent

apporter leur expertise de la recherche et de l'innovation dans le domaine de la cybersécurité.

Cette composition diversifiée du CP CSN permet une réflexion d'ensemble sur les différents aspects de la cybersécurité et favorise la coordination entre les différents acteurs au niveau national. Cela contribue à une mise en œuvre efficace de la CSN et à une meilleure protection de la Suisse contre les cyberincidents et les cybermenaces.

Al. 2 et 3 : Désignation des membres du CP CSN et de la présidence par le Conseil fédéral

Le Conseil fédéral désigne tous les cinq ans les membres du CP CSN, à l'exception des représentants des cantons, qui sont choisis par la Conférence des gouvernements cantonaux. Par la nomination régulière de membres tous les cinq ans, le Conseil fédéral garantit la participation de représentations actuelles et compétentes au CP CSN, qui disposent des connaissances techniques et des aptitudes nécessaires à la mise en œuvre efficace de la CSN. Cela contribue au caractère actuel et pertinent du comité. La nomination d'une présidence parmi les représentants de l'économie, de la société ou des hautes écoles souligne l'importance accordée à l'équilibre du comité. La présidence peut se faire l'écho de différents points de vue et garantir la prise en compte des intérêts des différents secteurs de façon appropriée. Globalement, cette structure permet un ajustement en continu aux nouvelles évolutions en matière de cybersécurité et favorise une participation équilibrée des différents groupes d'intérêt à la mise en œuvre de la CSN. Cela contribue à la mise en œuvre efficace de la CSN et à une meilleure protection de la Suisse contre les cyberincidents et les cybermenaces.

Art. 5 Tâches du CP CSN

La liste des tâches du CP CSN présentée à l'*art. 5* cible une mise en œuvre et une surveillance efficaces de la CSN. Voici son contenu :

- *Let. a :* le contrôle régulier de la CSN au moins une fois tous les cinq ans permet au comité de garantir l'adaptation de la stratégie aux évolutions de la situation et des menaces, ainsi que le développement afférent de cette stratégie. Au besoin, le comité peut émettre des recommandations concrètes ou réaliser des plans visant à adapter la CSN existante.

- *Let. b :* la définition de priorités et de calendriers pour la concrétisation des mesures permet d'engager les ressources efficacement et d'atteindre les objectifs de la stratégie.

- *Let. c :* l'évaluation régulière des progrès dans la concrétisation des mesures permet au comité de détecter précocement toute difficulté ou problème, d'y réagir en conséquence et d'informer le Conseil fédéral et les cantons de tout retard.

- *Let. d :* la formulation de propositions visant à compléter les mesures à l'intention du Conseil fédéral contribue à éliminer rapidement les obstacles.

- *Let. e :* le rapport annuel sur la concrétisation de la CSN assure la transparence et permet à tous les acteurs concernés de suivre la progression et de procéder éventuellement à des ajustements.

Section 3 Tâches de l'OFCS

Art. 6 Demande de renseignements aux titulaires

Cette disposition s'appuie sur l'art. 73*a*, al. 1 et 2, let. a, et l'art. 74, al. 1 et 2, let. a, LSI.

Jusqu'à fin 2023, la mission de l'OFCS en matière d'alerte du public était réglée à l'art. 12, al. 1, let. h, de l'OPCy abrogée. Depuis le 1er janvier 2024, elle est précisée à l'art. 15*a*, al. 2, let. d et e, Org-DDPS.

Depuis 2010, MELANI (Centrale d'enregistrement et d'analyse pour la sûreté de l'information), remplacée en 2020 par le NCSC puis par l'OFCS depuis le début de cette année, est considérée par l'Office fédéral de la communication (OFCOM) comme « un service de lutte contre la cybercriminalité reconnu par l'OFCOM » conformément à l'art. 15, al. 3, ODI[10] [11]. L'OFCS n'ayant pas de compétences ou de tâches relevant du droit pénal, il ne s'occupe qu'indirectement de cybercriminalité. De sorte à clarifier les compétences de l'OFCS pour requérir les coordonnées des titulaires de noms de domaine auprès du registre correspondant, ce pouvoir est évoqué expressément à l'*art. 6* (cf. à ce sujet l'art. 28*e,* let. b, LTC et les art. 7 ss ODI)[12]. La possibilité de requérir les coordonnées des titulaires de noms de domaine permet à l'OFCS, notamment dans le cas de cybermenaces aiguës ou de cyberattaques, d'avertir rapidement et de façon ciblée les parties potentiellement concernées et de les aider à mettre en œuvre des contre-mesures. Ce pouvoir est un instrument important de lutte contre les cybermenaces et les cyberattaques et de renforcement de la cybersécurité en Suisse.

Art. 7 Analyse technique des cyberincidents et des cybermenaces

Cette disposition s'appuie sur l'art. 73*a*, al. 1 et 2, let. a et e, ainsi que sur l'art. 74, al. 3, en relation avec l'art. 74*a*, al. 3, LSI.

---

10 Ordonnance du 5 novembre 2014 sur les domaines Internet (ODI ; RS **784.104.2**)

11 Cf. à ce sujet la page web de l'OFCOM « Lutte contre la cybercriminalité » (dernière consultation le 29 mars 2024).

12 L'OFCOM a confié à la fondation SWITCH l'affectation et l'administration des noms de domaine .ch (cf. art. 28*a*, al. 1, de la loi du 30 avril 1997 sur les télécommunications [LTC ; RS **784.10**] et art. 8, al. 2, en relation avec l'art. 33, ODI) que SWITCH administre dans une banque de données RDDS (WHOIS). L'OFCS a conclu un accord avec SWITCH qui règle la communication des noms des titulaires de domaine dans la banque de données RDDS (WHOIS) en ligne par l'accès RDAP.

Jusqu'à fin 2023, les tâches de l'équipe nationale d'intervention en cas d'urgence informatique (*Computer Emergency Response Team, CERT*) étaient réglées à l'art. 12, al. 1, let. c, de l'OPCy abrogée. Depuis le 1er janvier 2024, elles figurent à l'art. 15*a*, al. 2, let. f, Org-DDPS.

Al. 1 : Computer Emergency Response Team (CERT)

L'OFCS gère la CERT, qui joue un rôle central dans la gestion des cyberincidents et des cybermenaces en Suisse. La CERT est spécialisée dans la gestion des incidents sur le plan technique, l'analyse des questions techniques et l'identification et l'appréciation de cybermenaces d'un point de vue technique.

L'élément clé de l'analyse des questions techniques est la comparaison entre données provenant de cyberattaques et la recherche d'anomalies (let. a). À cet effet, la CERT développe ses propres instruments d'analyse et utilise des instruments d'analyse de tiers. Elle échange par ailleurs avec des spécialistes des équipes de sécurité de l'économie privée et d'autres pays.

L'OFCS procède à l'analyse technique de l'attaque (let. b) et contribue ainsi à la gestion des incidents. Cette analyse vise à comprendre le plus rapidement possible quelles méthodes d'attaque utilisent les attaquants, à quelles tactiques ils recourent et quels sont leurs objectifs. Ces informations permettent de déterminer et de mettre en œuvre des contre-mesures appropriées. L'OFCS collabore étroitement avec les autorités et les organisations concernées et leurs éventuels services de sécurité. Il contribue également à la coordination entre acteurs participant à la gestion technique. Au besoin, il peut aussi apporter son soutien directement sur place auprès de l'autorité ou de l'organisation concernée, à titre d'aide immédiate en cas d'urgence. Pour les travaux nécessaires à la restauration des données et à la reconstruction des systèmes après l'incident, l'OFCS fournit seulement des conseils.

La CERT apporte également une aide préventive aux autorités et aux organisations. Elle analyse en continu les nouvelles menaces techniques et méthodes d'attaque et identifie les contre-mesures appropriées (let. c). L'appréciation technique des menaces nécessite à la fois des outils automatisés d'analyse des cyberincidents et des cybermenaces, l'échange d'informations avec des services spécialisés nationaux et internationaux et l'expertise humaine requise pour interpréter les résultats. Cette veille continue permet de réagir de façon proactive aux dangers, de combler des failles de sécurité et d'adapter les stratégies de défense pour se protéger des cyberincidents et des cybermenaces actuels et futurs.

Al. 2 : Infrastructure résiliente

L'OFCS exploite une infrastructure résiliente qui doit fonctionner indépendamment du reste de l'informatique fédérale. De ce fait, l'OFCS est un prestataire pour cette infrastructure spécifique et dispose donc de ressources et de systèmes techniques particuliers pour analyser les cyberincidents et les cybermenaces.

L'infrastructure doit être indépendante en raison de la sensibilité et de l'urgence des cyberincidents et des cybermenaces. Premier interlocuteur national pour la cybersécurité, l'OFCS doit être en mesure d'analyser de façon fiable les

cyberincidents et les cybermenaces même lorsque le réseau informatique de la Confédération est défaillant.

Cette infrastructure indépendante et résiliente permet à l'OFCS d'accomplir efficacement ses tâches et de garantir que la Suisse puisse réagir de façon appropriée aux cyberincidents et aux cybermenaces.

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

Cette disposition s'appuie sur l'art. 74, al. 3, et l'art. 73*a,* al. 3, LSI.

Généralités :

L'art. 74, al. 3, LSI prévoit que l'OFCS puisse conseiller et soutenir les exploitants d'infrastructures critiques dans la gestion des cyberincidents et des cybermenaces et dans l'élimination des vulnérabilités, à condition que le fonctionnement de l'infrastructure critique concernée soit mis en péril et, s'il s'agit d'exploitants privés, qu'il ne soit pas possible d'obtenir en temps voulu un soutien équivalent sur le marché. Les entités concernées décident elles-mêmes si elles souhaitent faire appel au soutien de l'OFCS.

Le conseil et le soutien prennent principalement la forme d'analyses techniques et de renseignements sur des mesures techniques et organisationnelles. Les analyses techniques visent à identifier l'origine de l'incident, à comprendre l'ampleur du détournement et à identifier les potentielles vulnérabilités des moyens informatiques et du système de sécurité. Elles peuvent inclure par exemple un examen de journaux-système, des analyses de logiciels malveillants et des évaluations de la surveillance de réseaux. En plus des analyses techniques, l'OFCS peut conseiller des mesures organisationnelles afin de mieux gérer l'incident. Ayant travaillé sur de nombreux incidents, l'OFCS peut notamment indiquer comment l'on peut communiquer l'incident ou quelle organisation d'urgence est nécessaire.

Al. 1 : Priorité pour les services de conseil et d'assistance

L'al. 1 concerne une situation dans laquelle l'OFCS, en cas de cyberattaque, est confronté à un plus grand nombre de demandes de conseils et d'assistance que ce qu'il est capable de gérer avec les ressources humaines et techniques et les capacités disponibles. Dans un tel scénario, l'OFCS est en droit de décider quelles demandes seront traitées en premier et quelle sera l'ampleur de l'aide. Dans d'autres cas moins urgents, le conseil et l'assistance seront fournis de manière différée. Outre l'urgence, le degré d'aide fourni pourra également varier. Certains cas pourront exiger un examen complet et une assistance de grande ampleur, tandis que d'autres feront peut-être uniquement l'objet d'un conseil de base. Dans des périodes de forte activité, cette disposition permettra à l'OFCS de prendre des décisions stratégiques sur la meilleure façon d'utiliser ses ressources afin d'offrir la plus grande assistance possible.

Al. 2 : Priorité tenant compte des intérêts publics

Si plusieurs cyberincidents et cybermenaces se déclenchent simultanément, l'OFCS soutient en priorité les organisations et les autorités assujetties à l'obligation de signaler chez qui l'événement aura le plus d'incidences sur la sécurité, l'ordre public, le bien-être de la population ou le fonctionnement de l'économie. Ce traitement prioritaire signifie que l'OFCS mobilise ses ressources et son aide de façon ciblée sur les événements aux conséquences particulièrement graves. Ainsi, des infrastructures critiques, des établissements d'autorités ou d'autres organisations importantes peuvent être traités en priorité pour se voir garantir une protection appropriée et une assistance rapide en cas d'attaque. Par cette priorisation, l'OFCS veille à ce que les établissements et organisations les plus importants pour le fonctionnement de la société et de l'économie disposent d'une protection appropriée en cas de cyberincidents et de cybermenaces. Cela contribue à la résilience et à la stabilité du pays en cas d'événement de grande ampleur dirigé sur un grand nombre de cibles en Suisse.

Art. 9 Publication cordonnée des vulnérabilités

Cette disposition s'appuie sur l'art. 73*a*, al. 2, let. c, et l'art. 73*b*, al. 3, en relation avec l'art. 73*c*, al. 2, LSI.

L'OPCy ne réglait pas explicitement les tâches de l'OFCS en rapport avec la coordination des vulnérabilités. Depuis le 1er janvier 2024, les art. 15*a*, al. 2, let. b, Org-DDPS les mentionnent dans les tâches générales de l'OFCS. Par ailleurs, depuis lors, l'art. 43, al. 1, let. c, OSI contient une base légale pour la recherche de vulnérabilités dans l'infrastructure informatique de l'administration fédérale et de l'armée. Cette disposition prévoit que l'OFCS informe la Chancellerie fédérale, les secrétariats généraux, les départements et les offices fédéraux des menaces et des vulnérabilités actuelles et des risques qui les concernent et qu'il leur recommande si nécessaire des mesures de réduction des risques.

L'importance d'une gestion active des vulnérabilités et le rôle de l'OFCS dans la recherche et la publication coordonnée des vulnérabilités sont décrites plus en détail dans le rapport du Conseil fédéral « La promotion du piratage éthique en Suisse »[13].

Al. 1 : Divulgation cordonnée des vulnérabilités

La divulgation coordonnée des vulnérabilités est un élément important des efforts globaux de cybersécurité, car elle permet d'analyser de potentielles failles de sécurité dans les systèmes informatiques, de les évaluer et de les éliminer avant que des attaquants ne puissent les exploiter. L'objectif du processus de divulgation coordonnée est d'assurer un maximum de transparence sur les vulnérabilités, sans générer de risques pour la sécurité. L'élément clé du processus est de commencer par informer les fabricants sitôt une vulnérabilité détectée. Les hackers

[13] Cf. à ce sujet : Rapport du Conseil fédéral du 29 novembre 2023, La promotion du piratage éthique en Suisse, Rapport du Conseil fédéral en réponse au postulat 20.4594, Bellaiche, du 17 décembre 2020, ch. 4.2.4, p. 13 s.

conviennent avec ces derniers d'un délai au cours duquel ils ne diffuseront pas publiquement d'informations sur la vulnérabilité. Les fabricants disposent ainsi d'un laps de temps suffisant pour éliminer la vulnérabilité avant qu'elle ne soit rendue publique. Cette procédure est répandue à l'échelle internationale et est par exemple prescrite par l'UE dans la directive SRI 2 (art. 12 et 13)[14].

Les règles de divulgation coordonnée des vulnérabilités sont précisées dans la norme ISO/IEC 29147:2018-10[15]. L'OFCS doit divulguer les vulnérabilités signalées en suivant les règles énoncées dans cette norme. Cela signifie que l'OFCS ne tient aucune vulnérabilité secrète et qu'il ne la transmet pas à d'autres autorités sans en informer les fabricants. L'OFCS doit mettre en œuvre des mesures tout au long du processus de divulgation coordonnée qui empêcheront la mise à profit de la vulnérabilité.

En collaborant avec des services spécialisés étrangers et internationaux, l'OFCS s'assure que les vulnérabilités seront identifiées et éliminées au niveau international. En septembre 2021, l'organisation états-unienne MITRE a reconnu l'OFCS comme service spécialisé en vulnérabilités et l'a autorisé à attribuer aux vulnérabilités des numéros CVE conformément à la norme *Common Vulnerabilities and Exposure* (CVE), afin d'identifier sans aucune ambiguïté les vulnérabilités détectées. Ces numéros permettent aux experts en sécurité, fabricants, utilisateurs et autorités de se référer à une vulnérabilité de manière uniforme. L'utilisation de numéros CVE aide à communiquer, documenter et éliminer des failles de sécurité plus efficacement. L'utilisation d'un schéma de dénomination standardisé facilite aussi la collaboration entre les différents acteurs du domaine de la cybersécurité et améliore la transparence et l'efficacité dans le traitement de failles de sécurité.

Al. 2 à 4 : Délai d'élimination de la vulnérabilité

L'OFCS exige des fabricants du matériel informatique ou du logiciel concerné par la vulnérabilité qu'ils éliminent la vulnérabilité dans un délai de 90 jours. Il s'agit d'une pratique courante dans le secteur de la cybersécurité[16]. Ce délai laisse suffisamment de temps aux fabricants pour analyser les vulnérabilités et pour développer et mettre en œuvre des contre-mesures. Il garantit aussi que les vulnérabilités ne perdureront pas outre mesure.

Le délai peut être réduit quand le degré de criticité et la complexité de la vulnérabilité sont élevés, mais il peut aussi être prolongé au besoin (p. ex. en raison d'une charge importante liée aux contre-mesures ou d'un besoin de coordination accru).

---

14 Directive SRI 2. Directive (UE) 2022/2555 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)

15 ISO/IEC 29147:2018-10 (date de publication 2018-10), p. 14

16 Cf. directive de l'Office fédéral allemand pour la sécurité en matière de technologies de l'information au sujet du processus de Coordinated Vulnerability Disclosure (CVD), ch. 3.3, p. 10.

Al. 5 : Partage d'informations sur la vulnérabilité avant son élimination ou sa divulgation

S'il a connaissance d'une vulnérabilité qui représente une cybermenace aiguë pour d'autres infrastructures critiques, l'OFCS en informe leurs exploitants avant que la vulnérabilité ne soit publiée ou éliminée par le fabricant du matériel informatique ou du logiciel. Cette étape est importante pour informer à un stade précoce les exploitants d'infrastructures critiques de potentiels risques de sécurité et leur donner la possibilité de prendre des mesures adéquates pour protéger leurs systèmes. L'échange d'informations sur des vulnérabilités permet aux exploitants d'infrastructures critiques d'engager des mesures de réduction des risques de façon proactive avant que les vulnérabilités soient rendues publiques. Cela peut contribuer à empêcher ou atténuer de potentielles attaques sur des infrastructures critiques.

Al. 6 : Exception pour l'OFCOM

Cette disposition vise à éviter d'éventuels conflits de compétences et des doublons entre l'OFCS et l'OFCOM. L'OFCOM exerce la surveillance du marché sur l'offre, la mise à disposition sur le marché, la mise en service, la construction et l'exploitation d'installations de télécommunication. Pour ce faire, il effectue des contrôles de marché auprès des acteurs économiques, en premier lieu auprès du fabricant suisse ou, à défaut, de l'importateur, de telles installations, vérifie les installations concernées et prend les mesures nécessaires si les installations contrôlées ne respectent pas les prescriptions en vigueur (art. 33 de la loi sur les télécommunications du 30 avril 1997[17]; LTC). Parmi ces prescriptions figurent également les exigences en matière de cybersécurité pour certaines installations de radiocommunication, conformément à l'art. 7, al. 3, let. d, e et f, de l'ordonnance du 25 novembre 2015[18] sur les installations de télécommunication (OIT)[19].

Étant donné que les objectifs de l'OFCS et de l'OFCOM se recoupent à cet égard, la divulgation coordonnée visée au paragraphe 1 n'est pas réalisable si l'OFCOM découvre, avant l'OFCS et à l'occasion d'un contrôle d'un opérateur économique, une non-conformité d'un équipement de radiocommunication aux exigences en matière de cybersécurité. Dans la procédure de contrôle du marché, l'opérateur économique a connaissance, avant même le fabricant étranger, de l'existence d'une vulnérabilité dans les installations concernées, après l'examen de l'OFCOM. Il est donc nécessaire de mettre en place un mécanisme de coordination afin d'harmoniser les procédures de l'OFCOM et de l'OFCS. L'OFCOM informe en conséquence l'OFCS des vulnérabilités, lequel procède, le cas échéant, à la divulgation coordonnée des vulnérabilités conformément au paragraphe 1.

17 RS 784.10
18 RS 784.101.2
19 Les installations de radiocommunications concernées ne doivent pas avoir d'effets dommageables pour le réseau ou son fonctionnement, ni faire un usage abusif des ressources du réseau qui entraînerait une dégradation inacceptable du service. Elles doivent être dotées de dispositifs de sécurité destinés à protéger les données à caractère personnel et la vie privée des utilisateurs et des abonnés. Ils doivent également prendre en charge certaines fonctions de protection contre la fraude.

Al. 7 : Information de l'OFCOM

L'OFCOM a immédiatement besoin d'informations sur les vulnérabilités découvertes par l'OFCS dans les installations de télécommunication. Cela permet, d'une part, de garantir que l'OFCOM n'ouvre pas une procédure en même temps que la divulgation coordonnée de l'OFCS et, d'autre part, de permettre à l'OFCOM de déterminer, grâce à ces informations, la suite à donner à une procédure déjà en cours dans le cadre de sa surveillance du marché à l'encontre d'un fabricant ou d'un importateur suisse (voir à ce sujet les explications données plus haut au paragraphe 6).

Si le fabricant informé par l'OFCS a pu corriger la vulnérabilité dans le délai imparti, l'OFCOM peut ensuite vérifier si les adaptations du fabricant ont également été effectuées sur les installations disponibles sur le marché. Si la vulnérabilité n'a pas été corrigée, l'OFCOM peut prendre des mesures appropriées dans la procédure contre l'importateur.

Art. 10 Soutien aux autorités

Cette disposition s'appuie sur l'art. 73*a*, al. 2, let. c, LSI.

En tant que centre de compétences de la Confédération en matière de cybersécurité, l'OFCS appuie 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 notamment comme suit :

- *Expertise technique* : l'OFCS dispose de spécialistes qui peuvent conseiller et soutenir les autorités dans la mise en œuvre des normes et des réglementations sur la cybersécurité susmentionnées.

- *Mise à disposition d'un soutien technique* : l'OFCS soutient les autorités dans le développement et la mise en œuvre des normes et des réglementations sur la cybersécurité.

- *Coordination et collaboration* : l'OFCS se charge de la coordination pour faciliter la collaboration entre les différentes autorités et veille à ce que les normes et réglementations développées en matière de cybersécurité soient cohérentes et efficaces.

- *Échange d'informations* : l'OFCS sert de base pour l'échange sur les pratiques et les informations éprouvées dans le domaine de la cybersécurité entre autorités.

Section 4 Échange d'informations

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

Cette disposition s'appuie sur l'art. 73*a*, al. 1 et 2, let. e, et l'art. 74, al. 1 et 2, let. a, LSI.

Jusqu'à fin 2023, la tâche de l'OFCS en matière d'échange d'informations était réglée à l'art. 12, al. 1, let. b et i, de l'OPCy abrogée. L'Org-DDPS ne contient pas de disposition spécifique à ce sujet.

Al. 1 : Accès au système de communication sécurisé

Les attaquants utilisent souvent les mêmes méthodes et moyens dans leur attaques pour qu'elles réussissent auprès d'un maximum de victimes. Lorsque les victimes de cyberincidents et de cybermenaces appartenant à d'autres organisations et autorités communiquent rapidement à l'OFCS les enseignements qu'elles en ont tirés, le nombre de cyberincidents et de cybermenaces peut être nettement diminué. L'OFCS exploite à cet effet un système de communication permettant l'échange sécurisé d'informations sur les cyberincidents et les cybermenaces. Ce système permet à l'OFCS de communiquer rapidement et efficacement des informations sur des incidents et des menaces aux autorités et aux organisations enregistrées dont le siège est en Suisse. Ces dernières peuvent alors réagir plus vite à des menaces et prendre des contre-mesures. Par ailleurs, ce système de communication contribue aussi au développement d'une meilleure compréhension de la nature et de l'ampleur des cyberincidents et des cybermenaces.

Al. 2 : Responsabilité de l'OFCS en matière de sécurité et de protection des données

Le système de communication permettant l'échange sécurisé d'informations est un système d'information de l'OFCS. Ce dernier est responsable de la sécurité et veille à la légalité du traitement des données.

Art. 12 Systèmes d'information permettant l'échange automatique

Cette disposition s'appuie sur l'art. *73a*, al. 1 et 2, let. e, et l'art. 74, al. 1 et 2, let. a, LSI.

Al. 1 : Échange automatique d'informations

La mise à disposition de systèmes d'information par l'OFCS permettant l'échange automatique d'informations techniques est un moyen très important de protéger les infrastructures critiques des cyberincidents et des cybermenaces. Elle permet aux exploitants d'infrastructures critiques de toujours disposer des connaissances les plus récentes. L'OFCS utilise ces systèmes d'information protégés pour informer à un stade précoce les infrastructures critiques des indicateurs techniques et des schémas d'attaque qui ne sont pas encore connus du grand public et que l'OFCS ne peut

pas publier pour des raisons de sécurité. Les indicateurs techniques des cyberincidents ou des cybermenaces sont des indices spécifiques de menaces potentielles ou effectives dans le domaine des technologies de l'information et de la cybersécurité. Ils peuvent revêtir plusieurs formes, comme des signatures de maliciels avec des caractéristiques sans équivoque qui indiquent qu'un système est infecté ou a été exposé à une infection. Les anomalies dans le trafic réseau en font également partie. Il s'agit par exemple de schémas inhabituels au sein du trafic des données qui peuvent être le signe d'une éventuelle cybermenace, comme des taux de transfert de données anormalement élevés ou des connexions suspectes vers des adresses IP connues comme étant malveillantes. D'autres indicateurs de criminalistique numérique peuvent aussi être échangés automatiquement sur ces systèmes d'information avec les exploitants d'infrastructures critiques. Il peut s'agir de différents types de traces numériques qui laissent augurer d'un cyberincident ou d'une cybermenace, par exemple des modifications de fichier inhabituelles, des procédures d'identification suspectes ou des tentatives d'accès non autorisées. Lors de leur enregistrement auprès de l'OFCS, les exploitants d'infrastructures critiques sont enregistrés comme tels afin que l'OFCS puisse envoyer des informations techniques précitées ciblées uniquement au cercle des infrastructures critiques. Tous les exploitants d'infrastructures enregistrés sont attribués à un ou plusieurs secteurs de manière à permettre des échanges sectoriels.

Al. 2 : Responsabilité de l'OFCS en matière de sécurité et de protection des données

Par analogie avec les dispositions de l'art. 12, al. 2, l'OFCS est également responsable de la sécurité et de la protection des données des systèmes d'information permettant l'échange automatique d'informations.

Art. 13 Enregistrement

Cette disposition s'appuie sur l'art. 73*a*, al. 1 et 2, let. e, et l'art. 74, al. 1 et 2, let. a, LSI.

Al. 1 : Enregistrement en vue d'une participation à l'échange d'informations

Les organisations et les autorités intéressées sont tenues de s'enregistrer avant de pouvoir participer à l'échange d'informations et de communiquer sans délai à l'OFCS toute modification des données enregistrées.

Al. 2 : Données à enregistrer

L'enregistrement doit comporter au moins les informations suivantes :

- *Raison sociale, nom ou désignation et adresse de l'autorité ou de l'organisation (let. a)* : pour que les autorités et organisations puissent être identifiées correctement, elles doivent indiquer leur raison sociale, leur nom ou leur désignation et leur adresse avec les renseignements suivants : rue, numéro de bâtiment, numéro postal et localité.

- *Coordonnées de la personne ayant procédé à l'enregistrement (let. b) :* l'enregistrement des autorités ou des organisations doit comporter au moins le prénom et le nom de famille d'une personne de contact. Celle-ci doit également fournir son numéro de téléphone, son adresse e-mail et sa fonction. Plusieurs personnes de contact peuvent être enregistrées.

Au moment de l'enregistrement, l'autorité ou l'organisation est informée des prescriptions réglant la participation à un échange d'informations conformément à l'art. 15 OCyS ; leur enregistrement ne pourra être conclu qu'une fois que la personne aura confirmé activement avoir pris connaissance de ces prescriptions.

L'enregistrement pour la participation à l'échange d'informations n'est pas obligatoire, y compris pour les autorités et les organisations assujetties à l'obligation de signaler. S'enregistrer de façon précoce fera toutefois gagner du temps à ces entités concernées par l'obligation de signaler en cas de cyberattaque à signaler.

Art. 14 Fournisseurs de prestations

Cette disposition s'appuie sur l'art. 73*a*, al. 1 et 2, let. e, et l'art. 74, al. 1 et 2, let. a, LSI.

Al. 1 : *Annonce*

Pour garantir la sécurité et l'intégrité des infrastructures critiques en Suisse, les exploitants d'infrastructures critiques peuvent déclarer leurs fournisseurs de prestations de cybersécurité à l'OFCS conformément à l'*al. 1* afin que ceux-ci puissent participer aux échanges d'informations.

Al. 2 : Données à enregistrer

Les fournisseurs de prestations d'exploitants d'infrastructures critiques éventuellement déclarés doivent s'enregistrer conformément à l'*al. 2* en indiquant leur raison sociale ou leur nom ainsi que les coordonnées de la personne ayant procédé à l'enregistrement (cf. par analogie le commentaire de l'art. 13, al. 2, ci-dessus).

Art. 15 Transmission et utilisation des informations

Cette disposition s'appuie sur l'art. 73*a*, al. 1 et 2, let. e, et l'art. 74, al. 1 et 2, let. a, LSI.

Les informations sont échangées volontairement et sur la base de la confiance dans l'utilisation appropriée des informations fournies. Il est donc essentiel que les fournisseurs des informations puissent décider, dans le respect des dispositions légales, comment seront gérées les informations qu'ils partagent, et que tous les participants connaissent et respectent les prescriptions d'échange des informations.

Al. 1 : Transmission des informations partagées uniquement aux conditions des fournisseurs des informations

Il importe d'observer la règle selon laquelle les informations partagées ne peuvent être transmises (dans la mesure où la transmission des informations n'est pas prévue par la loi) qu'en conformité avec les conditions des fournisseurs des informations afin de garantir que celles-ci ne soient pas diffusées sans autorisation et qu'aucune utilisation abusive n'en soit faite. Les informations sur les cyberincidents et les cybermenaces doivent être partagées de façon confidentielle. Ces informations révèlent ce que l'on sait sur l'incident et quelles mesures de protection ont été identifiées. Les attaquants pourraient exploiter pareilles informations à leurs propres fins. De plus, ces informations incluent également des éléments sensibles pour l'autorité ou l'organisation concernée, par exemple parce qu'ils peuvent compromettre sa réputation. Il est donc important que les fournisseurs des informations puissent fondamentalement définir eux-mêmes le cercle des destinataires. En cybersécurité, la convention de classification *Traffic Light Protocol* (marquage TLP) s'est imposée à cet effet. Ce marquage initié par le *Forum of Incident Response and Security Teams* (FIRST)[20] distingue les niveaux suivants applicables à la diffusion des informations :

- TLP « clear » – diffusion publique, sans restriction.
- TLP « green » – les destinataires peuvent partager des informations, mais n'ont pas le droit de les diffuser publiquement.
- TLP « amber » – les destinataires peuvent partager des informations au sein de leur organisation[21] et avec leurs partenaires dans la mesure du nécessaire.
- TLP « amber strict » – les destinataires n'ont le droit de partager les informations qu'au sein de leur organisation.
- TLP « red » – l'information n'est transmise qu'à la personne concernée et ne doit pas être partagée.

Les informations partagées sur la plateforme de l'OFCS sont classées selon le *Traffic Light Protocol*. On y voit donc comment les informations peuvent être diffusées. Ces prescriptions sont contraignantes pour tous les destinataires, sauf si la transmission des informations est prévue par la loi.

Al. 2 : Décision de l'OFCS concernant la publication d'informations

L'OFCS a l'autorité de décider si des informations destinées à être transmises concernant des cybermenaces et des cyberattaques doivent être publiées, et à quel moment. Il est donc responsable de décider lesquelles de ces informations peut être communiquées à quels destinataires. Il s'agit ici d'informations examinées et

[20] Cf. à ce sujet Forum of Incident Response and Security Teams : Traffic Light Protocol (TLP), sur la page web Traffic Light Protocol (TLP) (first.org).

[21] Le TLP ne spécifie pas ce que recouvre le terme « leur organisation ». Dans les grandes entreprises ou les administrations en particulier, cela peut être source d'ambiguïtés. Dans l'administration, le protocole est mis en œuvre de sorte que le terme «organisation» renvoie à une unité administrative, p. ex. un office fédéral.

traitées en interne. On examine alors lesquelles sont utiles et pertinentes pour le grand public ou certains groupes cibles et de quelle manière il est préférable de les diffuser via le système de communication existant ou les systèmes d'information.

Al. 3 : Garantie de la protection des informations

Les destinataires des informations ont la responsabilité d'engager des mesures visant à en garantir la sécurité et la confidentialité. La protection de ces informations est particulièrement importante, car il peut s'agir de données sensibles et leur publication ou détournement pourrait avoir des conséquences négatives, par exemple favoriser d'autres cyberattaques ou aggraver des problèmes de sécurité existants.

Al. 4 : Prescriptions pour les éventuels fournisseurs de prestations d'exploitants d'infrastructures critiques

Les fournisseurs de prestations qui travaillent pour des infrastructures critiques et qui ont été déclarés et enregistrés par les exploitants d'infrastructures critiques conformément à l'art. 14 OCyS ont le droit d'utiliser les informations qu'ils reçoivent uniquement aux fins des activités spécifiques qu'ils exécutent dans le cadre de l'infrastructure critique. Cela permet de garantir la confidentialité et la gestion appropriée des informations sensibles, mais aussi de réduire à un minimum le risque d'utilisation abusive ou d'accès non autorisé.

Section 5 Obligation de signaler

Art. 16 Exceptions à l'obligation de signaler

Cette disposition s'appuie sur l'art. 74*c* LSI en vertu duquel le Conseil fédéral exempte des autorités et des organisations de l'obligation de signaler visée à l'art. 74*b* LSI lorsque les perturbations provoquées par des cyberattaques n'ont qu'un effet limité sur l'ordre public, la sécurité, le bien-être de la population ou le fonctionnement de l'économie.

Généralités :

Si des autorités ou des organisations sont assujetties à l'obligation de signaler en vertu de l'art. 74*b* LSI dans plusieurs domaines, l'exemption dans un domaine ne les dispense pas de l'obligation de signaler dans la mesure où elles sont encore assujetties à ladite obligation dans un ou plusieurs autres domaines.

Il faut également noter que certaines autorités et organisations assujetties à l'obligation de signaler ne sont pas concernées par des exceptions à ladite obligation visées aux al. 1 et 2 expliqués ci-après. En font partie :

- les organisations qui fournissent des prestations destinées à couvrir les conséquences de la maladie, des accidents, de l'incapacité de travail et de gain, de la vieillesse, de l'invalidité et de l'impotence (art. 74*b*, al. 1, let. i, LSI) ;

- la Société suisse de radiodiffusion et télévision (art. 74*b*, al. 1, let. j, LSI), et

- les agences de presse d'importance nationale (art. 74*b*, al. 1, let. k, LSI).

Al. 1 : Seuils spécifiques

Des exceptions spécifiques aux domaines ne sont pas définies au niveau de la loi afin que le Conseil fédéral puisse adapter rapidement les seuils fixés au niveau de l'ordonnance en cas d'évolutions. Dans la mesure du possible, les seuils ont été définis en fonction des défis spécifiques de chaque domaine.

Let. a : Organes visés à l'art. 74b, al. 1, let. b et c, LSI

Par *« organes visés à l'art. 74b, al. 1, let. b et c, LSI »*, on entend ceci :

- Les autorités fédérales, cantonales et communales et les organisations intercantonales, cantonales et intercommunales (art. 74*b*, al. 1, let. b, LSI) responsables de moins de 1000 résidents permanents sont exemptées de l'obligation de signaler. Les administrations généralement petites, voire très petites, de ces communes sont épargnées afin de ne pas leur imposer une charge de travail supplémentaire. Avec ce seuil de 1000 résidents permanents, près de 40 % des communes sont exemptées de l'obligation de signaler, soit environ 430 000 résidents.

- Les organisations chargées de tâches de droit public dans les domaines de l'approvisionnement en eau potable, du traitement des eaux usées et de l'élimination des déchets dont les activités se limitent au niveau communal ou à une organisation responsable de moins de 1000 résidents permanents sont exemptées de l'obligation de signaler.

L'exception ne s'applique pas aux fournisseurs et aux exploitants de services et d'infrastructures servant à l'exercice des droits politiques visés à l'art. 74*b,* al. 1, let. s, LSI. Ceux-ci sont également assujettis à l'obligation de signaler lorsqu'ils proposent des services et des infrastructures pour moins de 1000 résidents.

Let. b : Entreprises visées à l'art. 74b, al. 1, let. d, LSI

Les seuils définis ici pour le domaine de l'électricité s'appuient sur l'ordonnance du 14 mars 2008 sur l'approvisionnement en électricité (OApEl)[22], qui déclare comme contraignantes les recommandations de la norme minimale pour améliorer la résilience informatique[23] pour certains acteurs de la branche de l'électricité[24]. Elle

[22] RS **734.71**

[23] Office fédéral pour l'approvisionnement économique du pays, « Norme minimale pour améliorer la résilience informatique », Berne, 2018

[24] Le 21 septembre 2023, le Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC) a lancé la consultation sur les révisions partielles de plusieurs ordonnances dans le domaine de l'énergie. Il est prévu que la révision de l'ordonnance sur l'approvisionnement en électricité (OApEl) renforce la protection face aux cybermenaces dans l'approvisionnement en électricité. À cet effet, la norme minimale TIC est déclarée contraignante pour les principaux acteurs de l'approvisionnement en électricité – gestionnaires de réseau, producteurs et exploitants de stockage. Ils sont rattachés à un certain niveau de protection (profil de protection) correspondant à des exigences échelonnées à atteindre.

prévoit que les acteurs doivent atteindre un certain niveau de protection de leurs installations face aux cybermenaces dans la mise en œuvre de la norme minimale (niveau de protection A, B ou C). Le niveau de protection dépend de la taille et de l'influence de l'acteur sur la sécurité d'approvisionnement et est défini par des seuils. De ce fait, seules les entreprises d'électricité des deux niveaux de protection les plus élevés A et B sont soumises à l'obligation de signaler. Les acteurs plus petits, qui doivent se conformer aux exigences moins strictes du niveau de protection C, sont exemptés de l'obligation de signaler. Les producteurs d'électricité et les exploitants de stockage d'électricité sont acteurs du droit sur l'approvisionnement en électricité, comme les gestionnaires de réseau[25]. Dans la mesure où une entreprise exploite des installations pour la production et pour le stockage d'électricité et que ces installations se commandent à distance par le même système, les prestations s'additionnent. Les prestataires des gestionnaires de réseau, des producteurs d'électricité et des exploitants de stockage sont eux aussi concernés par la règle sur les exemptions. Ne font pas partie de ces prestataires les fabricants de matériel informatique ou de logiciels visés à l'art. 74*b*, al. 1, let. u, LSI, pour qui il n'y a pas de règle d'exemption.

Le seuil de 400 GWh/an défini à l'*art. 16, al. 1, let. b, ch. 2,* OCyS pour les exploitants de gazoducs a été défini en collaboration avec l'Association suisse de l'industrie gazière (ASIG). C'est la quantité totale d'énergie transitant par leur réseau (vers les consommateurs finaux ou vers d'autres réseaux) qui est déterminante. La règle d'exemption ne concerne que les exploitants de gazoducs ayant pour activité la vente de gaz aux consommateurs finaux (Transitgas SA, p. ex., ne serait pas concerné par la clause sur les exemptions).

L'art. 74*b*, al. 1, let. d, LSI précise que l'obligation de signaler s'applique aux entreprises œuvrant dans l'approvisionnement en électricité et en gaz mais aussi à d'autres entreprises travaillant dans l'énergie, comme les exploitants de conduites transportant du pétrole, les entreprises de chauffage à distance, les raffineries ou les entreprises des secteurs du bois-énergie et du charbon. Ces entreprises sont soumises à l'obligation de signaler, sauf si elles ne dépassent pas les seuils définis à l'art. 16, al. 2, let. b OCyS. Les entreprises actives à la fois dans l'approvisionnement en électricité ou en gaz et dans un autre secteur de l'énergie (pétrole, chauffage à distance, etc.) ne peuvent se prévaloir d'une règle d'exemption que si la cyberattaque ou ses conséquences se limitent à ce secteur de l'énergie.

Sont d'ores et déjà exemptés de l'obligation de signaler conformément à l'art. 74*b,* al. 1, let. d, LSI les détenteurs d'une autorisation au sens de la loi du 21 mars 2003 sur l'énergie nucléaire[26]. Une réglementation au niveau de l'ordonnance est donc superflue.

Let. c : *Entreprises visées à l'art. 74b, al. 1, let. n, LSI*

Les entreprises visées à l'art. 74*b,* al. 1, let. n, LSI et qui ne doivent satisfaire à aucune prescription spécifique de gestion de la sécurité ou de programme

[25] Au sujet des producteurs d'électricité, cf. art. 5, al. 2, de la loi du 23 mars 2007 sur l'approvisionnement en électricité (LApEl ; RS **734.7**). Au sujet des exploitants de stockage d'électricité, cf. p. ex. art. 17*a*, al. 1, LApEl ou art. 8*a*, al. 1, let. a, ch. 3, OApEl.

[26] RS **732.1**

conformément aux règlements européens cités sont exemptées de l'obligation de signaler à l'OFCS les cyberattaques ciblant leurs systèmes informatiques. Cela s'applique aux entreprises qui :

- ne sont pas tenues d'installer un système management de la sécurité de l'information (SMSI) selon les art. 2 et 4 et l'annexe II du règlement d'exécution (UE) 2023/203 du 5 octobre 2023 ou l'art. 2 et l'annexe II du règlement délégué (UE) 2022/1645 du 14 juillet 2022. Celles-ci sont également exemptées de l'obligation de signaler les cyberattaques à l'OFCS. Un SMSI est une approche systématique de gestion d'informations sensibles concernant des entreprises, de sorte qu'elles restent sûres. Il englobe des personnes, des processus et des systèmes informatiques par la mise en œuvre d'un processus de gestion du risque. Les règlements européens précités définissent les normes et les exigences en vigueur pour la mise en place d'un tel système,

- qui ne sont pas tenues d'appliquer les conditions du point 1.7 de l'annexe du règlement d'exécution (UE) 2015/1998, qui concerne les règles de sécurité pour l'aviation civile. Le point 1.7 de l'annexe pourrait comporter des mesures ou des normes spécifiques de sécurité qui devraient être mises en œuvre dans un programme de sûreté. Si l'entreprise concernée n'est pas tenue de mettre en œuvre ces conditions dans son programme de sûreté – ce qui s'effectue sur la base des art. 2, 12, 13 ou 14 du règlement (CE) 300/2008 – elle est également exemptée de l'obligation de signaler en cas de cyberattaques.

Let. d : Entreprises ferroviaires visées à l'art. 74b, al. 1, let. m, LSI

L'obligation de signaler se limite aux entreprises de transport surveillées par l'OFT dont les tâches systémiques relèvent de l'intérêt public et dont le fonctionnement sûr et fiable est indispensable au bien-être de la population et au fonctionnement de l'économie. De ce fait, les autres entreprises sont exemptées de l'obligation de signaler.

Let. e : Fournisseurs et exploitants visés à l'art. 74b, al. 1, let. t, LSI

Les fournisseurs et les exploitants d'informatique en nuage, de moteurs de recherche et de centres de calcul dont le siège est en Suisse sont assujettis à l'obligation de signaler uniquement s'ils fournissent tout ou partie de leurs prestations à des tiers et contre rémunération. La mise en place du critère de fourniture de prestations à titre commercial exclut donc de l'obligation de signaler les centres de calcul qui fournissent leurs services uniquement pour couvrir les propres besoins.

De même, tous les services numériques de sécurité et tous les services numériques de confiance proposés à des tiers sont assujettis à l'obligation de signaler des cyberattaques quels que soient leur chiffre d'affaires et leur clientèle (sans seuil moyen). En revanche, les services qu'une personne développe et utilise uniquement pour ses propres besoins ne sont pas soumis à l'obligation de signaler.

Al. 2 : Seuils communs à plusieurs secteurs

Concernant l'obligation de signaler à laquelle sont soumises entreprises, la valeur seuil en catégorie d'entreprise prise comme exception générale est « petite entreprise », conformément à la recommandation de la Commission de l'UE[27]. De ce fait, les autorités et les organisations assujetties à l'obligation de signaler visées à l'art. 74*b* LSI sont exemptées de cette obligation lorsqu'elles emploient moins de 50 personnes et que leur chiffre d'affaires ou leur bilan annuel ne dépasse pas 10 millions de francs. Il n'y aura pas de conversion d'euros en francs suisses, car la règle européenne s'applique aussi pour des pays de l'UE plus faibles économiquement et où le chiffre d'affaires ou le bilan annuel de 10 millions d'euros est plus difficile à atteindre.

La dispense visée à l'al. 2 ne vaut que pour les entreprises assujetties à l'obligation de signaler pour lesquelles aucun seuil spécifique n'a été défini à l'al. 1. En font partie :

- les établissements de santé figurant sur la liste hospitalière cantonale conformément à l'art. 39, al. 1, let. e, de la loi fédérale du 18 mars 1994 sur l'assurance-maladie[28] (art. 74*b,* al. 1, let. f, LSI),

- les laboratoires médicaux titulaires d'une autorisation conformément à l'art. 16, al. 1, de la loi du 28 septembre 2012 sur les épidémies[29] (art. 74*b,* al. 1, let. g, LSI),

- les entreprises titulaires d'une autorisation de fabriquer, de mettre sur le marché ou d'importer des médicaments conformément à la loi du 15 décembre 2000 sur les produits thérapeutiques[30] (art. 74*b,* al. 1, let. h, LSI),

- les prestataires de services postaux enregistrés auprès de la Commission de la poste conformément à l'art. 4, al. 1, de la loi du 17 décembre 2010 sur la poste[31] (art. 74*b*, al. 1, let. l, LSI), et

- les entreprises qui approvisionnent la population en biens d'usage quotidien indispensables et dont la défaillance partielle ou complète entraînerait de graves difficultés d'approvisionnement (art. 74*b*, al. 1, let. p, LSI).

Il convient de souligner ici que l'exception citée à l'al. 2 ne concerne pas les autorités fédérales, cantonales et communales (art. 74*b*, al. 1, let. b, LSI) ni les hautes écoles (art. 74*b*, al. 1, let. a, LSI).

27 Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (2003/361/CE)
28 RS **832.10**
29 RS **818.101**
30 RS **812.21**
31 RS **783.0**

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

Cette disposition s'appuie sur l'art. 74*a,* al. 2, LSI.

L'obligation de signaler concernant de très nombreux domaines différents d'après la liste dressée à l'art. 74*b,* al. 1, LSI et un grand nombre d'autorités et d'organisations étant exemptées de cette obligation en vertu de l'art. 74*c* LSI et de l'art. 16 OCyS, il faut s'attendre, malgré ces règles détaillées, à ce que certaines autorités et organisations s'interrogent sur le fait qu'elles soient ou non concernées par l'obligation de signaler. Les autorités et les organisations intéressées peuvent s'adresser à l'OFCS pour savoir si elles sont assujetties à l'obligation de signaler au sens de l'art. 74*b* LSI ou si elles en sont exemptées au sens de l'art. 74*c* LSI.

Pour permettre à l'OFCS de traiter cette demande de renseignements, l'*art. 17* prévoit que les autorités et les organisations lui fassent parvenir l'ensemble des documents requis pour qu'il puisse indiquer si celles-ci sont assujetties à une obligation légale de signaler. Cette exigence permet de s'assurer que l'OFCS puisse remplir efficacement ses missions dans le domaine de la cybersécurité. Le renseignement fourni par l'OFCS étant quasiment un instantané basé sur les faits valables au moment où il est établi, il incombe à l'autorité ou à l'organisation concernée de s'acquitter sans délai de son obligation de signaler en cas de changement significatif des faits ou des circonstances pertinentes ou, en cas de doute, de se renseigner auprès de l'OFCS.

Art. 18 Cyberattaques à signaler

Cette disposition s'appuie sur l'art. 74*d* LSI.

Généralités :

La description des cyberattaques à signaler est précisée à l'art. 74*d*, let. a à d, LSI. Les cyberattaques sont à signaler lorsqu'elles sont particulièrement pertinentes pour l'OFCS à des fins d'alerte précoce et d'évaluation de la menace. Les critères de détermination des attaques à signaler ont été choisis de manière à ce que les autorités et les organisations puisse les identifier le plus rapidement possible. Cet article permet de les préciser au niveau de l'ordonnance.

Al. 1 : Mise en péril du fonctionnement de l'infrastructure critique (art. 74d, let. a, LSI)

Le fonctionnement d'une infrastructure critique peut être mis en péril par une cyberattaque quand les systèmes informatiques, les réseaux ou les systèmes de pilotage essentiels à l'exploitation de l'infrastructure sont compromis à tel point que les collaborateurs et tiers sont touchés par des interruptions de système (art. 18, al. 1, let. a) ou que l'organisation ou l'autorité touchée ne peut maintenir ses activités qu'à l'aide de plans d'urgence (art. 18, al. 1, let. b). On parle d'interruption de système lorsque les collaborateurs ou les tiers ne peuvent plus exécuter des étapes de travail importantes pour leur activité car les moyens informatiques nécessaires ne sont

plus disponibles. Les plans d'urgence sont des mesures techniques ou organisationnelles à prendre lorsque les moyens informatiques habituellement utilisés ne sont plus disponibles subitement de façon inattendue.

Al. 2 : Manipulation ou fuite d'informations (art. 74d, let. b, LSI)

Il y a cyberattaque assujettie à l'obligation de signaler faisant suite à une manipulation ou à une fuite d'informations lorsque les attaquants sont en mesure d'accéder de manière non autorisée à des données sensibles des organisations ou des autorités concernées et de les modifier, chiffrer, voler, effacer, communiquer ou rendre accessibles à des tiers non autorisés. À la suite d'une cyberattaque, des données peuvent être manipulées par des tiers non autorisés de façon à entrer dans les systèmes des informations importantes pour les affaires visées à l'art. 18, al. 2, let. a, OCyS qui, du fait de leur modification ou communication, entraînent des erreurs dans les processus commerciaux, la prise de décisions erronées, voire des risques pour la sécurité. Il est aussi possible, conformément à l'art. 18, al. 2, let. b, OCyS, que la manipulation ou la fuite d'informations aboutisse à la violation de la sécurité de données personnelles selon l'art. 5, let. h, en relation avec l'art. 24 LPD.

Al. 3 : Cyberattaque indétectée pendant une période prolongée (art. 74d, let. c, LSI)

Doivent également être signalées les cyberattaques indétectées pendant une période prolongée, avec des indices qui laissent penser qu'elles ont été exécutées en vue de préparer d'autres attaques. L'art. 18, al. 3, OCyS précise que l'on parle de période prolongée au sens de l'art. 74*d*, let. c, LSI quand on se rend compte après la découverte que la cyberattaque a eu lieu plus de 90 jours auparavant (p. ex. par l'analyse des fichiers journaux). Pareilles cyberattaques constituent une menace sérieuse pour les infrastructures critiques. Elles sont aussi souvent qualifiées d'*Advanced Persistent Threats* (APT). Il s'agit généralement de cyberattaques très perfectionnées, ciblées et difficiles à identifier. De ce fait, elles sont particulièrement pertinentes pour mettre en garde d'autres exploitants d'infrastructures critiques. Avec ce type d'attaques, l'espionnage ne peut pas être exclu (p. ex. espionnage des autorités ou industriel). Souvent très complexes, les attaques sont effectuées par des attaquants expérimentés qui utilisent des techniques et des outils avancés pour se cacher dans le système et dissimuler leurs activités. Les cibles sont en général des organisations, des secteurs d'activité ou des autorités spécifiques. Il arrive aussi que les attaquants avancent progressivement pour étendre les droits d'accès et exploiter d'autres vulnérabilités. Si des indices laissent à penser qu'une cyberattaque a été exécutée en vue de préparer d'autres attaques, il est probable que les attaquants aient déjà accédé à des systèmes ou à données critiques qu'ils pourront les utiliser dans de futures attaques.

Al. 4 : Cyberattaque liée à des actes de chantage, de menace ou de contrainte (art. 74d, let. d, LSI)

Cet alinéa précise que, lors de circonstances susceptibles d'entraîner des poursuites pénales, une cyberattaque doit toujours être signalée lorsque les actes répréhensibles sont dirigés contre l'autorité ou l'organisation assujettie à

l'obligation de signaler, d'actuels ou d'anciens responsables, d'actuels ou d'anciens collaborateurs ou encore des personnes travaillant pour l'autorité ou pour l'organisation assujettie à l'obligation de signaler. De nombreux cybercriminels tentent, par la menace ou la réalisation d'attaques, de faire chanter les exploitants d'infrastructures critiques, leur clientèle ou des membres de leur personnel (p. ex. en chiffrant des données à l'aide de rançongiciels ou en les menaçant de compromettre la disponibilité par des attaques de *Distributed Denial of Service* [attaques DDoS] ou de publier des informations sensibles comme des données personnelles ou des secrets d'entreprise). Les cyberattaques s'accompagnant de circonstances susceptibles d'entraîner des poursuites pénales doivent être signalées quand l'acte de chantage, la menace ou l'acte de contrainte se rapportent à l'organisation ou à l'autorité assujettie à l'obligation de signaler et peuvent porter préjudice à leur activité professionnelle ou administrative. Il s'agit ici de conséquences graves, associées à des pertes financières, une atteinte à la réputation ou des répercussions juridiques. Il est important de signaler pareilles attaques afin que l'OFCS puisse évaluer la menace que font peser les cybercriminels sur les infrastructures critiques.

Art. 19 Contenu du signalement

Cette disposition s'appuie sur l'art. 74*e*, al. 2, LSI.

Généralités :

La rédaction de cette disposition d'exécution s'appuie largement sur la terminologie et le contenu du formulaire mis en place par la FINMA au 1er septembre 2020 qui concerne l'« obligation de signaler les cyberattaques »[32]. L'OFCS n'ayant pas de fonction de surveillance, contrairement à la FINMA, certains éléments n'ont pas été repris, car ils ne sont pas significatifs dans le cadre de l'obligation de signaler à l'OFCS. Ainsi, aucune indication sur les fonctions critiques ou sur les mesures de communication n'est demandée lors du signalement à l'OFCS, car ces informations n'apportent pas de valeur ajoutée à l'évaluation de la cyberattaque ou à la mise en garde d'éventuelles victimes. Par ailleurs, des éléments importants issus du formulaire sur les incidents de sécurité informatique de l'Office fédéral allemand pour la sécurité en matière de technologies de l'information (BSI) ont été repris pour l'analyse des cyberattaques[33]. Le formulaire d'annonce de violation de la sécurité des données[34] que reçoit le PFPDT a également servi d'inspiration pour l'obligation de signaler des cyberattaques.

L'art. 74*e*, al. 2, LSI fixe le contenu du signalement, c'est-à-dire les principales informations nécessaires pour satisfaire à l'obligation de signaler. L'étendue concrète et la teneur des informations à signaler sont précisées dans la présente disposition

---

32 Cf. communication FINMA sur la surveillance 05/2020 du 7 mai 2020 fondée sur l'art. 29, al. 2, de la loi du 22 juin 2007 sur la surveillance des marchés financiers (LFINMA ; RS **956.1**) et a été précisée par la FINMA dans la circulaire 2023/1 (circ.-FINMA 2023/1, ch. marg. 68).

33 Cf. formulaire de signalement d'événements en rapport avec la sécurité informatique sur le portail d'annonce et d'information de l'Office fédéral allemand pour la sécurité en matière de technologies de l'information.

34 Cf. service en ligne d'annonce de violation de la sécurité des données (art. 24 LPD).

d'exécution et reprises par l'OFCS dans un formulaire sur son système de communication. Ce formulaire décrit en détail les informations à indiquer.

Par ailleurs, il est rappelé que pour s'acquitter de l'obligation de signaler envers l'OFCS, il n'est pas nécessaire de fournir des informations qui concernent ou violent d'éventuels secrets professionnels, d'éventuels secrets d'affaires ou qui exposent à des poursuites pénales (cf. art. 74*e*, al. 4, LSI).

Al. 1 : Informations sur le type et l'exécution de la cyberattaque

Le signalement au sens de l'*al. 1* contient les informations suivantes sur le type et l'exécution de la cyberattaque :

- *Date et heure de la constatation de l'attaque (let. a) :* le signalement doit indiquer à quel moment (date et heure) la cyberattaque a été découverte.

- *Date et heure de l'attaque (let. b) :* la date et l'heure de l'attaque doivent aussi être indiquées dans le signalement. Si elles ne sont pas connues, l'heure supposée de la cyberattaque peut être indiquée.

- *Type d'attaque (let. c) :* concernant le type et l'exécution de la cyberattaque, le formulaire de signalement prévoit les types d'attaque les plus courants (p. ex. DDoS, accès non autorisé, maliciel, abus / utilisation inadéquate de l'infrastructure technologique, etc.). La cyberattaque peut aussi être décrite dans une zone de texte du formulaire.

- *Méthode d'attaque (let. d) :* les méthodes d'attaque (ou vecteurs d'attaque dans le jargon technique) les plus fréquentes sont les attaques par phishing, l'exploitation de vulnérabilités, les attaques par saturation des serveurs, le vol d'identité, etc. Le formulaire de signalement prévoit les vecteurs d'attaque les plus fréquents. Plusieurs réponses sont possibles et des méthodes ou vecteurs peuvent être ajoutés.

- *Données sur l'agresseur (let. e) :* l'identification des auteurs d'une cyberattaque peut être une tâche complexe et délicate, car les attaquants essaient souvent de dissimuler leurs traces et de rester anonymes. Mais il existe plusieurs types d'informations qui peuvent contribuer à identifier les auteurs d'une cyberattaque comme les adresses IP, les données DNS, l'URL de pages suspectes, les valeurs de hachage de maliciels, les signatures de virus, les anomalies dans le trafic réseau ou le comportement suspect d'un logiciel. Si elles sont disponibles, ces informations doivent être jointes au signalement.

Al. 2 : Informations sur l'éventualité d'un chantage, d'une menace ou d'une contrainte en lien avec l'attaque et sur une éventuelle dénonciation des faits

La publication d'actes de chantage ou de menace en lien avec une cyberattaque peut contribuer à mettre en garde d'autres victimes potentielles et à prendre des mesures de prévention face à de telles situations. Comme un acte de chantage, de menace ou de contrainte en lien avec une cyberattaque peut avoir des conséquences

pénales, les autorités et les organisations assujetties à l'obligation de signaler dénoncent parfois les faits. L'OFCS pourra réagir de façon plus appropriée s'il sait que les faits ont été dénoncés.

Al. 3 : Informations sur les conséquences de la cyberattaque
Les informations à fournir selon l'*al. 3*, *let. a à c*, aident l'OFCS à effectuer une première évaluation des conséquences de la cyberattaque et du préjudice porté aux moyens informatiques et aux données.

- *Unités touchées de l'organisation ou de l'autorité (let. a) :* dans les grandes entreprises, les conglomérats et les groupes aux nombreux domaines d'activité en particulier, citer l'unité touchée par la cyberattaque aide l'OFCS à évaluer si les moyens informatiques et les données de l'infrastructure critique sont touchés.

- *Gravité du préjudice sur la disponibilité, l'intégrité et la confidentialité des informations propres et de celles de tiers (let. b) :* l'autorité et l'organisation assujetties à l'obligation de signaler doivent évaluer à quel point la disponibilité, l'intégrité et la confidentialité sont touchées par la cyberattaque visant les moyens informatiques. Selon l'évaluation des conséquences de la cyberattaque, un degré de gravité sera affecté au préjudice subi avec la qualification « faible, moyen, élevé ou grave », comme sur le formulaire de signalement de la FINMA[35]. Sur la base de cette première évaluation des conséquences et de l'attribution d'un degré de gravité, on peut dans certains cas identifier si une tendance se dessine pour ce qui est des conséquences. Cette information est particulièrement utile en présence d'indices d'aggravation. Par ailleurs, cette classification nourrit aussi la prise de décision lorsque l'aide de l'OFCS est demandée concernant la suite concrète à donner pour gérer l'incident.

- *Effets sur le fonctionnement des unités touchées de l'autorité ou de l'organisation (let. c) :* les indications sur les effets de la cyberattaque sur le fonctionnement de l'autorité ou de l'organisation doivent révéler à quel point sont notamment touchés l'accès aux systèmes et aux données, la disponibilité des services pour les clients ou les citoyens, les déroulements internes, les processus, la disponibilité des systèmes d'approvisionnement en électricité et en eau, les services de santé ou d'autres infrastructures critiques. L'autorité ou l'organisation assujettie à l'obligation de signaler peut également s'exprimer sur l'intervalle de temps et la durée des répercussions de la cyberattaque et donner son pronostic sur la durée des conséquences de cette dernière.

Al. 4 : Informations sur l'autorité ou l'organisation assujettie à l'obligation de signaler

Dans la mesure où l'autorité ou l'organisation assujettie à l'obligation de signaler n'est pas déjà enregistrée pour participer à l'échange d'informations et où l'enregistrement est impossible au moment d'effectuer le signalement (p. ex. en raison d'une

[35] Cf. à ce sujet l'annexe 1 de la communication FINMA sur la surveillance 05/2020 du 7 mai 2020, p. 7.

défaillance des moyens informatiques) ou que l'autorité ou l'organisation assujettie à l'obligation de signaler ne souhaite pas le faire, le signalement d'une cyberattaque conformément à l'*al. 4* doit aussi contenir les informations suivantes sur ladite autorité ou organisation :

- *Raison sociale, nom ou désignation et adresse de l'autorité ou l'organisation assujettie à l'obligation de signaler (let. a)* : pour une identification correcte des autorités et des organisations assujetties à l'obligation de signaler, celles-ci doivent indiquer leur raison sociale, leur nom ou leur désignation ainsi que leur adresse avec les renseignements suivants : rue, numéro de bâtiment, numéro postal et localité.

- *Coordonnées de l'auteur du signalement (let. b)* : le signalement doit comporter au moins le prénom et le nom de l'auteur du signalement. Son numéro de téléphone et son adresse e-mail doivent également être indiqués, car il est la personne de contact de l'OFCS. Les organisations ou les autorités peuvent déclarer plusieurs personnes de contact.

Art. 20 Transmission du signalement

Cette disposition s'appuie sur l'art. 74*f* LSI.

Conformément à l'*art. 20,* l'OFCS confirme immédiatement la réception du signalement à l'autorité ou à l'organisation assujettie à l'obligation de signaler si ce signalement n'a pas été fait par le système de communication de l'OFCS. Si le signalement est effectué par exemple par e-mail, l'OFCS informe les personnes de contact de l'autorité ou l'organisation assujettie à l'obligation de signaler qui se sont enregistrées au préalable conformément à l'art. 13, al. 2, let. b, OCyS. Ce retour garantit que l'autorité et l'organisation assujettie à l'obligation de signaler puissent communiquer à l'OFCS qu'il s'agissait d'une fausse alerte (p. ex. « canular » par des tiers).

Art. 21 Délai de saisie du signalement

Cette disposition s'appuie sur l'art. 74*e*, al. 1 et 3, LSI.

Généralités :

Les autorités et les organisations assujetties à l'obligation de signaler doivent signaler immédiatement toute cyberattaque dès qu'elle est connue, le principe étant que la rapidité prévaut sur l'exhaustivité, car l'OFCS doit être prévenu immédiatement de toute cyberattaque à signaler afin de remplir son mandat légal d'alerte précoce.

Al. 1 : Complément ou modification du signalement

Puisqu'il est essentiel pour l'alerte précoce et la prévention en particulier que les cyberattaques soient signalées dès leur découverte par les autorités et les

organisations assujetties à l'obligation de signaler, l'art. 74*e,* al. 1, LSI fixe un délai de signalement de 24 heures. Le délai commence à courir une fois la cyberattaque détectée. Les informations connues jusqu'alors doivent être communiquées pendant ce laps de temps. Lors de cyberattaques, on met très souvent beaucoup de temps à en déterminer la gravité et à savoir ce qui s'est passé précisément. Si les éléments demandés par l'OFCS à l'art. 19 OCyS ne sont pas connus dans leur intégralité au moment du signalement, les personnes touchées peuvent compléter le signalement avec les éléments manquants une fois qu'elles ont obtenu de nouvelles informations ou qu'elles connaissent suffisamment bien la situation. Elles peuvent aussi confirmer l'indisponibilité de ces informations. Ces précisions doivent être transmises à l'OFCS dans les 14 jours suivant le signalement de la cyberattaque. Ces deux délais ne peuvent pas être prolongés, car il s'agit de délais légaux (cf. art. 22, al. 1, PA).

Al. 2 : Requête de l'OFCS

Si l'autorité ou l'organisation assujettie à l'obligation de signaler ne communique pas les informations requises sur la cyberattaque dans les 14 jours prescrits, l'OFCS lui demande de compléter immédiatement le signalement ou de confirmer que ces informations ne sont pas disponibles.

Section 6 Dispositions finales

Art. 23 Entrée en vigueur

L'ordonnance entre en vigueur le 1er janvier 2025, en même temps que la LSI révisée.

3 Modification d'autres actes

1. Ordonnance du 7 mars 2003 sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports

Art. 15*a,* al. 2, let. f, Org-DDPS

Comme l'art. 7 de cette ordonnance décrit plus en détail les tâches de l'équipe d'intervention en cas d'urgence informatique (*Computer Emergency Response Team* [CERT]) de l'OFCS, l'actuel art. 15*a,* al. 2, let, f, Org-DDPS est réduit en conséquence afin d'éviter les doublons.

Art. 15*a,* al. 2, let. h, Org-DDPS

L'art. 15*a,* al. 2, let. h, Org-DDPS prévoit que l'OFCS représente la Suisse pour l'analyse technique des cybermenaces et la gestion des cyberincidents dans des instances internationales. Cette mention est importante car les cyberincidents et les cybermenaces sont des phénomènes internationaux. Les attaquants utilisent simultanément les mêmes technologies et méthodes dans de nombreux pays.

L'échange national et international entre services spécialisés est donc indispensable pour se protéger des cyberincidents et des cybermenaces. L'OFCS échange activement des informations sur ce sujet avec des services nationaux et internationaux qui assument des tâches semblables à celles de l'OFCS. Cet échange d'informations sert à partager des connaissances et des données importantes sur les menaces actuelles et à coordonner des mesures communes de gestion des cyberincidents et des cybermenaces. Ainsi, par rapport aux États de l'UE, l'OFCS, avec sa CERT, occupe le rang de *Computer Security Incident Response Team* (centre de réponse aux incidents de sécurité informatique, CSIRT), comme prescrit par la directive SRI 2 de l'UE pour tous les États membres de l'UE[36]. Par ailleurs, l'OFCS représente la Suisse au sein d'organes internationaux dans le cadre technique de l'analyse des cyberincidents et des cybermenaces et de la gestion des incidents. Cela signifie que l'OFCS participe à des forums et groupes de travail internationaux afin de partager ses connaissances techniques et ses expériences dans le domaine de la cybersécurité et de bénéficier du savoir d'autres pays. Par le partage de données et la participation à des comités internationaux, l'OFCS aide la Suisse à s'informer des dernières évolutions dans le domaine de la cybersécurité et à profiter des bonnes pratiques d'autres pays. La capacité de l'OFCS à réagir de façon appropriée aux cyberincidents et aux cybermenaces et également à contribuer à la sécurité globale s'en trouve renforcée. Toutes ces tâches exigent un échange d'informations avec des services suisses, étrangers et internationaux dont les bases légales sont précisées à l'art. 73*d,* al. 1, et aux art. 76, 76*a* et 77, LSI.

2. Ordonnance du 31 août 2022 sur la protection des données

Art. 41, al. 1, OPDo

Le Parlement ayant adopté le 29 septembre 2023 une modification de la LSI selon laquelle une obligation de signaler les cyberattaques contre les infrastructures critiques serait mise en place au 1er janvier 2025, l'art. 41, al. 1, de l'ordonnance du 31 août 2022 sur la protection des données doit être abrogé en raison des modifications décidées.

[36] Directive (UE) 2022/2555 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)