Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

22.xxx

Message 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)

du …

Madame la Présidente,
Monsieur le Président,
Mesdames, Messieurs,

Par le présent message, nous vous soumettons le projet d'une modification de la loi sur la sécurité de l'information visant à y inscrire une obligation de signaler les cyberattaques contre les infrastructures critiques, en vous proposant de l'adopter.

Nous vous prions d'agréer, Madame la Présidente, Monsieur le Président, Mesdames, Messieurs, l'assurance de notre haute considération.

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Ignazio Cassis
Le chancelier de la Confédération, Walter Thurnherr

Condensé

Contexte

Ces dernières années, les cyberincidents se sont multipliés, que ce soit chez les particuliers, dans les entreprises ou même au sein des autorités, avec, parfois, des conséquences graves.

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 contre les infrastructures critiques.

Une telle obligation permettra de détecter précocement les cyberattaques, d'analyser le mode opératoire utilisé et d'avertir à temps les autres exploitants d'infrastructures critiques. Elle pourra ainsi apporter une contribution essentielle au renforcement de la cybersécurité de la Suisse. Le Conseil fédéral a ouvert la consultation sur l'avant-projet le 12 janvier 2022. Les résultats de la consultation ont été intégrés dans le projet.

Contenu du projet

Non seulement le projet établit l'obligation de signaler les cyberattaques contre les infrastructures critiques, mais il ancre aussi dans la loi les tâches du Centre national pour la cybersécurité (NCSC), créé en 2019. Il règle en particulier la fonction de guichet unique qui est attribuée au NCSC et qui consiste à réceptionner les signalements obligatoires de cyberincidents, de même que les signalements volontaires de cyberincidents et de vulnérabilités des moyens informatiques.

L'obligation de signaler est mise en place pour les cyberattaques perpétrées par des tiers non autorisés qui visent intentionnellement des infrastructures critiques. Le signalement d'une cyberattaque n'est cependant obligatoire que si l'attaque a des conséquences graves, comme la mise en péril du fonctionnement de l'infrastructure critique touchée.

Table des matières

Message

1 Contexte

L'introduction d'une obligation de signaler les cyberattaques revient régulièrement dans les discussions. Ce sujet a gagné en importance à la suite de l'adoption de la directive (UE) 2016/1148[1] (directive SRI), qui introduit une telle obligation. Le Conseil fédéral a examiné en plusieurs étapes si la mise en place d'une telle obligation en Suisse était nécessaire et réalisable. Sur la base des résultats de ces travaux, il a décidé de préparer un projet de loi.

1.1 Nécessité d'agir et objectifs visés

Dans son rapport du 13 décembre 2019 en réponse au postulat «Infrastructures critiques. Prévoir une obligation de signaler les incidents graves de sécurité», le Conseil fédéral a constaté qu'il n'existait pas d'obligation de signaler les cyberincidents dont sont victimes les infrastructures critiques[2] et a chargé le Centre national pour la cybersécurité (NCSC) d'étudier la possibilité d'introduire une telle obligation.

Ce mandat d'examen reposait sur des bases solides telles que la stratégie nationale pour la protection des infrastructures critiques (stratégie PIC 2018-2022, mesure 8) et la stratégie pour la protection de la Suisse contre les cyberrisques (SNPC 2018-2022, mesure 9), ainsi que sur le rapport du groupe d'experts concernant le traitement et la sécurité des données[3]. La question d'introduire une obligation de signaler a aussi été soulevée dans le cadre des débats parlementaires concernant la révision totale de la loi fédérale sur la protection de la population et sur la protection civile (LPPCi, délibérations au Conseil national du 14 juin 2019) et dans le cadre de ceux concernant la loi sur la sécurité de l'information (LSI, débat au Conseil national du 4 juin 2020). Après un examen approfondi des bases légales possibles et, plus particulièrement, de la compétence fédérale[4], le Conseil fédéral a, le 11 décembre 2020, chargé le Département fédéral des finances (DFF) d'élaborer d'ici à la fin 2021 un projet destiné à la consultation prévoyant l'introduction d'une obligation de signaler les cyberattaques contre des infrastructures critiques.

1 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, JO L 194 du 19.7.2016, p. 1.

2 Obligation de déclarer les incidents graves affectant la sécurité des infrastructures critiques: solutions possibles. Rapport du Conseil fédéral du 13 décembre 2019 en réponse au postulat 17.3475 Graf-Litscher du 15 juin 2017

3 Rapport du groupe d'experts du 17 août 2018 concernant le traitement et la sécurité des données (recommandation 28). Le groupe d'experts a été engagé par le DFF le 27 août 2015 dans le cadre de la mise en œuvre de la motion Rechsteiner (13.3841) «Commission d'experts pour l'avenir du traitement et de la sécurité des données», pour un mandat limité à trois ans.

4 Rapport du 25 novembre 2020 «Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen, Rechtliche Grundlagen», annexe 01 au mandat du Conseil fédéral du 11 décembre 2020 (disponible en allemand uniquement)

Ce projet visait à clarifier qui doit signaler quels types d'attaques, quand et à qui. Lors de la clarification de ces questions, il est apparu clairement que le NCSC, créé en 2019 – et que le projet institue comme guichet de signalement des cyberattaques – ne disposait pas des bases légales nécessaires pour accomplir ses tâches de centre de compétence fédéral pour la cybersécurité conformément aux exigences du Parlement[5]. Le projet visant à introduire une obligation de signaler servira donc aussi à ancrer dans la loi les tâches et les compétences du NCSC.

1.2 Solutions étudiées et solution retenue

L'obligation de signaler est un instrument qui déploie des effets immédiats et permet de garantir la communication des informations sur les cyberattaques à un service centralisé. Mais d'autres options sont possibles. Le Conseil fédéral a étudié, d'une part, si le développement de l'échange d'informations à titre volontaire permettrait d'obtenir un résultat aussi efficace et, d'autre part, s'il serait possible d'étendre les obligations de déclaration existantes afin qu'elles englobent aussi les cyberattaques, plutôt que de créer une nouvelle obligation.

Il apparaît qu'aucune de ces variantes n'apporterait une solution satisfaisante, raison pour laquelle il a été décidé de créer une nouvelle obligation de signaler, qui devra être mise en œuvre au moyen d'incitations et de sanctions.

1.2.1 Première option écartée: développement de l'échange d'informations à titre volontaire

En Suisse, l'échange d'informations entre les infrastructures critiques et la Confédération est bien en place. Les infrastructures critiques procèdent à des échanges depuis 2004, à l'époque avec la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), aujourd'hui avec le NCSC. Les limites de ce système se font toutefois de plus en plus ressentir. Un échange réciproque nécessite une relation de confiance entre toutes les parties intéressées. Pour établir une telle relation, il faut que le nombre de participants reste gérable et que ceux-ci aient la possibilité d'échanger directement de façon régulière. Dans la situation actuelle, où les cyberattaques constituent une menace pour une multitude d'entreprises actives dans les secteurs critiques, il n'est plus possible de garantir qu'une confiance mutuelle suffisante anime tous les opérateurs concernés. De fait, ces dernières années, l'échange d'informations est resté limité à un cercle d'entreprises et d'organisations avec lesquelles la collaboration est bien établie et continue de donner satisfaction. Mais compte tenu du nombre élevé d'infrastructures critiques qui sont exposées à des cybermenaces, il n'est plus réaliste d'envisager l'extension de ce modèle.

L'accent mis sur quelques entreprises promptes à communiquer des cyberincidents, qui est la conséquence directe du caractère facultatif des signalements, peut donner une image incomplète, voire biaisée, de la situation. Il est en effet impossible de déterminer quel est le rayon d'action en Suisse d'une cybermenace. Par ailleurs, l'échange d'informations à titre volontaire peut constituer une incitation inopportune. Les entreprises qui n'y prennent pas part reçoivent tout de même des alertes et des indications techniques grâce aux signalements d'autres sociétés, puisque le NCSC ne

5 17.3508 Mo. Eder «Création d'un centre de compétence fédéral pour la cybersécurité»

peut pas priver les exploitants d'infrastructures critiques d'informations essentielles. Il peut donc sembler plus facile à certaines entreprises de se reposer sur la participation des autres pour recevoir les signalements importants plutôt que de participer activement à l'échange d'informations.

En définitive, l'introduction d'une obligation de signaler est donc préférable à la poursuite de l'échange facultatif d'informations: elle assure une vue d'ensemble plus complète de la situation et garantit qu'aucun opérateur ne se soustraie à l'obligation d'avertir les autres de tout incident ou danger. Il s'agira néanmoins d'entretenir la culture de la collaboration née de l'échange d'informations, ainsi que la confiance mutuelle. Pour y parvenir, il faut aussi que l'introduction de l'obligation de signaler apporte une plus-value aux entreprises et aux organisations concernées.

1.2.2 Deuxième option écartée: extension d'obligations de déclaration existantes et échange d'informations entre autorités

La possibilité d'intégrer l'obligation de signaler les cyberattaques dans des obligations de déclaration existantes a aussi été examinée, car cela permettrait de renoncer à l'introduction d'une nouvelle obligation de signaler intersectorielle. Cette option a été rejetée en raison de l'absence de réglementation relative aux incidents de sécurité dans certains secteurs et du manque d'homogénéité des règles dans les secteurs où il y en a. Le travail nécessaire pour compléter et coordonner les obligations de déclaration existantes et pour régler l'échange d'informations entre les autorités concernées aurait été plus important que l'introduction d'une nouvelle obligation de signaler et aurait conduit à des processus inefficients.

L'obligation de signaler les cyberattaques ne remplace pas les obligations de déclaration existantes, mais les complète. On a veillé à ce que les bases légales puissent permettre de remplir simultanément différentes obligations de déclaration, et ce, afin de réduire au minimum la charge de travail liée à leur exécution. Cela concerne surtout – mais pas uniquement – l'obligation d'annonce visée à l'art. 24 de la loi fédérale du 25 septembre 2020 sur la protection des données révisée (nLPD)[6], étant donné que, dans la pratique, les cyberattaques entraînent fréquemment des pertes de données. L'option retenue offre la possibilité à l'auteur du signalement d'une cyberattaque de transmettre simultanément son annonce au NCSC et, en tout ou en partie, à d'autres guichets de signalement, afin de satisfaire à d'autres obligations de déclaration. Cette possibilité évitera aux victimes de cyberattaques de devoir signaler le même incident à plusieurs services selon des procédures différentes.

Lorsque des entreprises et des organisations signalent des cyberattaques au NCSC, que ce soit à titre volontaire ou pour satisfaire à l'obligation de signaler, elles doivent être au clair sur ce qu'il adviendra de leur signalement et sur les personnes qui en prendront connaissance. Les principes de l'échange d'informations appliqués jusqu'ici avec MELANI doivent aussi perdurer dans cette perspective. Toute transmission d'un signalement, complète ou partielle, doit impérativement être approuvée par les parties concernées ou être effectuée sous une forme anonymisée (art. 73*d*, al. 1).

6 RS **235.1**; RO **2022** 491

Le NCSC est toutefois autorisé à transmettre sans leur accord des informations permettant d'identifier les auteurs du signalement ou les entités concernées dans deux cas. Premièrement, une transmission aux autorités de poursuite pénale est possible si le signalement contient des informations sur une infraction grave. Cela ne vaut donc que pour des cas exceptionnels, car le personnel du NCSC est en principe exempté de l'obligation de dénoncer prévue à l'art. 22*a* de la loi du 24 mars 2000 sur le personnel de la Confédération (LPers)[7]. Le directeur du NCSC peut toutefois transmettre des informations aux autorités de poursuite pénale s'il estime que la gravité de l'infraction le justifie (art. 73*d*, al. 3).

Le deuxième cas de transmission autorisée concerne les informations pertinentes pour le Service de renseignement de la Confédération (SRC) dans le cadre de l'accomplissement de ses tâches, à savoir la détection précoce et la prévention des menaces pour la sûreté intérieure ou extérieure, l'appréciation de la menace ou le service d'alerte précoce en vue de protéger les infrastructures critiques, conformément à l'art. 6, al. 1, let. a, 2 et 5, de la loi fédérale du 25 septembre 2015 sur le renseignement (LRens)[8]. Cela permet de garantir que le SRC, en sa qualité d'autorité compétente pour l'alerte précoce concernant les infrastructures critiques et pour l'appréciation de la menace, reçoive les informations pertinentes en matière de sécurité (art. 73*d*, al. 2).

1.2.3 Solution retenue: obligation de signaler mise en œuvre au moyen d'incitations et de sanctions

Parallèlement à l'introduction de l'obligation de signaler se pose la question des outils permettant de la mettre en œuvre. Trois facteurs peuvent influencer la disposition des entités à se soumettre à cette obligation.

Premièrement, effectuer un signalement doit être aussi simple que possible. Le NCSC s'en assure en mettant à disposition un formulaire électronique au moyen duquel le signalement est rapide à saisir et facile à transmettre.

Deuxièmement, le fait de signaler un incident doit comporter des avantages (incitation positive): le NCSC offre notamment une évaluation technique et apporte un soutien subsidiaire dans la gestion de l'attaque. Cette aide est proposée en guise de «premier secours» et ne doit pas concurrencer des prestations disponibles sur le marché. Pour les intéressés, il peut toutefois s'avérer très utile de bénéficier de l'appui d'un organe fédéral qui a une vue d'ensemble de la situation et des menaces pour obtenir une première appréciation et mettre en œuvre des mesures d'urgence. Les autorités et organisations satisfont à l'obligation de signaler peuvent prétendre à ce soutien.

Le troisième facteur consiste à mettre en place une incitation négative sous la forme d'une amende: si un exploitant d'infrastructure critique viole l'obligation de signaler malgré une prise de contact et un rappel à l'ordre, il doit être possible de sanctionner ce comportement.

En lieu et place d'une amende, il aurait été envisageable de publier le nom des assujettis défaillants. Cette variante a toutefois été écartée, car cela ne serait pas propice

7 RS **172.220.1**
8 RS **121**

au climat de confiance nécessaire à la bonne collaboration entre les assujettis à l'obligation de signaler et le NCSC. Une autre possibilité aurait été que le NCSC refuse d'apporter son soutien à la gestion d'un incident lorsque l'assujetti est défaillant. Cette variante a elle aussi été écartée pour des questions liées à la politique de sécurité: sa mise en œuvre nécessiterait en effet d'accepter, dans certaines circonstances, des conséquences graves pour l'économie et la société.

Le seul instrument qui reste à disposition pour sanctionner un assujetti défaillant est donc la possibilité que le NCSC rende, en dernier recours, une décision dont le non-respect est passible de l'amende. Le montant maximal de l'amende est fixé à 100 000 francs, dont 20 000 francs peuvent être directement à la charge de l'entreprise qui exploite l'infrastructure critique. Sur la base de la longue collaboration avec les infrastructures critiques, le Conseil fédéral part du principe que cette disposition a plutôt un caractère symbolique et sert surtout à garantir que l'obligation de signaler reçoive l'attention requise.

1.3 Relation avec le programme de la législature et avec le plan financier, ainsi qu'avec les stratégies du Conseil fédéral

Le projet a été annoncé dans le message du 29 janvier 2020 sur le programme de la législature 2019 à 2023[9] et dans l'arrêté fédéral du 21 septembre 2020 sur le programme de la législature 2019 à 2023[10]. Le message soulignait notamment la nécessité de pouvoir identifier et maîtriser rapidement les cyberincidents affectant les infrastructures critiques, ainsi que celle d'augmenter la résilience informatique. L'objectif 18, visé à l'art. 19 de l'arrêté fédéral, précise quant à lui que «la Confédération combat les cyberrisques; elle soutient et prend des mesures visant à protéger les citoyens et les infrastructures critiques». Le message comme l'arrêté fédéral renvoient à la stratégie nationale du 18 avril 2018 de protection de la Suisse contre les cyberrisques pour les années 2018 à 2022.

Le budget 2022 avec plan intégré des tâches et des finances pour les années 2023 à 2025[11] définit comme une priorité stratégique l'amélioration de la cybersécurité au sein de la Confédération et en Suisse et mentionne l'obligation des infrastructures critiques de signaler les cyberattaques parmi les affaires relatives aux objectifs du Conseil fédéral. Il y est précisé que le NCSC contribue à la protection de la Suisse contre les cyberrisques.

9 FF **2020** 1709 p. 1797
10 FF **2020** 8087 p. 8094
11 Tome 2B – Budget 2022 avec PITF 2023–2025 des unités administratives 2e partie (DFF, DEFR, DETEC), p. 11 ss (www.efv.admin.ch > FR > Rapports financiers > Budget assorti d'un plan intégré des tâches et des finances)

2 Procédure de consultation

2.1 Projet envoyé en consultation

Le 12 janvier 2022, le Conseil fédéral a pris connaissance de l'avant-projet et du rapport explicatif, et a chargé le DFF d'ouvrir une procédure de consultation. L'avant-projet propose une modification du chapitre 5 de la LSI, qui contient déjà des dispositions sur la cybersécurité des infrastructures critiques. En plus des modifications de la LSI, l'avant-projet prévoit aussi d'apporter des changements à la nLPD[12], à la loi du 23 mars 2007 sur l'approvisionnement en électricité (LApEl)[13] et à la loi fédérale du 21 juin 2019 sur les marchés publics (LMP)[14].

Les dispositions générales (section 1) inscrivent dans la loi les tâches de la Confédération dans le domaine de la protection contre les cybermenaces. Après la création du NCSC, dans le cadre des décisions du 30 janvier 2019 sur l'organisation de la Confédération en matière de cyberrisques[15], il est apparu nécessaire de créer des bases légales spécifiques régissant les activités du NCSC.

L'art. 73*a* définit les tâches fondamentales du NCSC. Il est complété à l'art. 74 par la description du soutien que le NCSC peut apporter aux exploitants d'infrastructures critiques. Dans la perspective de la mise en place d'une obligation de signaler, l'art. 73*b* décrit les tâches du NCSC en sa qualité de guichet de signalement des cyberincidents et des vulnérabilités, tandis que les art.73*c* et 73*d* précisent quelles informations contenues dans les signalements le NCSC est habilité à transmettre, à quel moment et à qui.

L'avant-projet établit le principe selon lequel le NCSC ne peut pas publier ou communiquer des informations sur les cyberincidents qui contiennent des données personnelles ou des données sur des personnes morales sans un consentement explicite. Il reste néanmoins possible de transmettre à d'autres autorités ou au public des évaluations et analyses statistiques tirées des signalements reçus. L'art. 73*d* délimite les exceptions à ce principe. Premièrement, le NCSC transmet au SRC les informations provenant de signalements dont ce dernier a besoin pour remplir son mandat légal d'appréciation de la menace et d'alerte précoce des exploitants d'infrastructures critiques. Deuxièmement, si les informations obtenues dans le cadre du signalement ou de son analyse fournissent des indications sur une éventuelle infraction, elles peuvent être transmises aux autorités de poursuite pénale à la discrétion du directeur du NCSC, si la gravité de l'infraction éventuelle le justifie. Ce cas de figure doit rester exceptionnel, raison pour laquelle les membres du personnel du NCSC ne sont pas soumis à l'obligation de dénoncer prévue à l'art. 22*a* LPers si, dans le cadre du signalement d'un cyberincident ou de son analyse, ils obtiennent des informations sur une infraction éventuelle.

12 RS **235.1**; RO **2022** 491
13 RS **734.7**
14 RS **172.056.1**
15 Cf. Communiqué du Conseil fédéral du 31.01.2019 « Le Conseil fédéral donne le coup d'envoi à la création du Centre de compétences pour la cybersécurité »

La section 2 crée l'obligation de signaler les cyberattaques contre des infrastructures critiques. L'art. 74*a* oblige les infrastructures critiques à signaler au NCSC les cyberattaques visant leurs moyens informatiques. L'art. 74*b* définit ensuite le cercle des assujettis à cette obligation en énumérant concrètement les domaines dans lesquels l'obligation de signaler s'applique. Enfin, l'art. 74*c* charge le Conseil fédéral de restreindre le cercle des assujettis dans certains domaines, afin d'exempter les organisations de moindre importance de l'obligation de signaler. L'art. 74*d* décrit les types de cyberattaques qui doivent être signalés et les art. 74*e* et 74*f* déterminent les délais que doivent respecter les auteurs des signalements, les informations qu'ils doivent fournir ainsi que les modalités de la transmission des signalements. Enfin, les art. 74*g* et 74*h* fixent la procédure et les conséquences que risquent les assujettis s'ils ne respectent pas leurs obligations en matière de signalement des cyberattaques.

Pour terminer, l'avant-projet prévoit la modification de trois autres actes. La nLPD est adaptée afin que le préposé fédéral à la protection des données et à la transparence (PFPDT) puisse bénéficier des connaissances spécialisées du NCSC lors de l'examen d'annonces de violations de la sécurité des données. Dans la LApEl, une base légale est créée pour qu'il soit possible de forcer les gestionnaires de réseau, les producteurs et les agents de stockage à prendre des mesures pour protéger adéquatement leurs installations contre les cybermenaces. Une disposition est ajoutée dans la LMP afin de contraindre les soumissionnaires qui n'éliminent pas dans le délai imparti une vulnérabilité du matériel informatique ou du logiciel qu'ils ont fabriqué à répondre de ce manquement dans le cadre du droit des marchés publics.

2.2 Aperçu des résultats de la procédure de consultation

La consultation a duré du 12 janvier 2022 au 14 avril 2022. Le département compétent a reçu 99 avis (25 cantons, 4 conférences cantonales, 7 partis politiques, 5 associations faîtières, 39 organisations intéressées, 19 entreprises)). La proposition d'introduire une obligation de signaler les cyberattaques contre les infrastructures critiques a été très largement approuvée par les participants à la procédure de consultation. Pour 89 d'entre eux, dont tous les cantons, l'orientation générale du projet est positive, mais quelques réserves ont été émises. Le projet est explicitement rejeté par 7 participants, dont un parti politique, une association faîtière de l'économie suisse, 2 organisations intéressées, 2 entreprises et une personne physique.

Les réserves des participants qui approuvent le projet visent essentiellement les points suivants.

– *Charge de travail pour les intéressés:* la charge de travail liée à l'exécution de la nouvelle obligation de signaler doit rester aussi faible que possible pour les intéressés. La saisie des signalements doit être simple et il doit être possible de saisir plusieurs obligations de signaler semblables via un seul processus (guichet de signalement ou one-stop shop).

– *Sanctions en cas d'infraction:* le principe des sanctions est rejeté par 24 participants. Ces derniers estiment que l'obligation de signaler ne doit pas être mise en œuvre au moyen d'amendes, mais d'incitations. Des sanctions iraient à l'encontre du but poursuivi, qui est de favoriser les échanges d'informations entre la Confédération et le secteur privé.

– *Définition trop large des cyberattaques:* l'avant-projet inclut les tentatives d'attaques dans la définition des cyberattaques (art. 5) et ne délimite pas clairement les cyberattaques soumises à l'obligation de signaler (art. 74d). Pour 23 participants, cette délimitation doit être plus claire et plus stricte. D'une manière générale, ils souhaitent que les termes (cyberattaque, cyberincident, cybermenace, cyberrisques) soient définis plus clairement et utilisés de manière plus rigoureuse.

– *Étendue du champ d'application de l'obligation de signaler:* les domaines énumérés à l'art. 74b ne sont pas tous délimités assez clairement, ce qui pourrait entraîner une insécurité juridique quant à l'application de l'obligation de signaler. Des modifications de cet article sont demandées par 39 participants, la plupart d'entre elles concernant une délimitation plus stricte des domaines, soit dans la loi, soit dans l'ordonnance.

– *Transmission d'informations:* 6 participants ont critiqué la possibilité de communiquer des informations provenant de signalements aux autorités de poursuite pénale ou au SRC. Ils demandent que cette transmission ne soit possible que sous une forme anonymisée. Le canton de Berne et la Conférence des commandants des polices cantonales de Suisse demandent quant à eux que le NCSC soit tenu de transmettre tous les signalements aux autorités de poursuite pénale.

– *Loi sur la transparence:* pour 6 participants, il faut que les activités du NCSC, et plus précisément les signalements, soient explicitement exclues du champ d'application de la loi du 17 décembre 2004 sur la transparence (LTrans)[16].

En plus de ces réserves, les participants à la procédure de consultation ont proposé de compléter le projet avec les points suivants.

– *Normes minimales et compétence du NCSC de donner des instructions:* la prévention des cyberincidents ne devrait pas uniquement passer par une obligation de signaler, mais également par l'introduction de normes minimales sur la cybersécurité des infrastructures critiques. En outre, 9 participants souhaitent que le NCSC puisse donner des instructions en matière de cybersécurité aux exploitants d'infrastructures critiques.

– *Impunité pour les pirates éthiques:* l'activité des pirates éthiques, qui recherchent activement des vulnérabilités dans le but de les signaler aux intéressés, est une contribution précieuse à la cybersécurité. Certains participants exigent que le signalement des vulnérabilités soit encouragé et que les pirates éthiques puissent bénéficier de l'impunité pour leurs activités.

– *Fabricants négligents:* CH++ propose une procédure plus cohérente vis-à-vis des fabricants qui, en dépit d'une sommation du NCSC, n'éliminent pas les vulnérabilités de leurs logiciels ou de leur matériel informatique. Concrètement, leur négligence devrait pouvoir être prise en considération dans le cadre des contrats ou des procédures d'adjudication en cours.

16 RS **152.3**

2.3 Appréciation des résultats de la procédure de consultation

Grande acceptation de l'obligation de signaler

La mise en place d'une obligation de signaler ainsi que la désignation du NCSC en tant que guichet de signalement national et la clarification des tâches de la Confédération en matière d'analyse des signalements et de soutien subsidiaire aux exploitants d'infrastructures critiques sont accueillies favorablement. Le projet est qualifié d'étape importante vers l'amélioration de la cybersécurité en Suisse, car il règle explicitement la compétence de la Confédération en cas de cyberincidents. De nombreux participants à la procédure de consultation relèvent toutefois que la terminologie utilisée doit être précisée. En particulier, le projet utilise souvent le terme «cyberrisque» sans que cette notion soit clairement définie. La liste des définitions a donc été remaniée et le terme «cyberrisque» a été remplacé par celui de «cybermenace».

Rôle du NCSC

De nombreux participants ont proposé d'étendre le rôle du NCSC. Celui-ci devrait ainsi être doté de la compétence de donner des instructions aux exploitants d'infrastructures critiques, ce qui pourrait par exemple inclure la compétence d'exiger le respect de normes minimales en matière de sécurité ou d'ordonner directement l'élimination d'une vulnérabilité. Cette proposition n'a pas été reprise. Le but du projet est de favoriser l'alerte précoce des exploitants d'infrastructures critiques et les échanges d'informations avec eux. Si le NCSC devait être doté de fonctions de régulation et de surveillance, il se pourrait que les entreprises ne soient plus aussi disposées à partager des informations avec lui, y compris sur une base volontaire.

Charge de travail et utilité pour les assujettis à l'obligation de signaler

Bien qu'une majorité de participants à la procédure de consultation salue l'introduction d'une obligation de signaler, plusieurs réserves ont été exprimées. Pour les cantons, mais également pour les milieux économiques, il est important que l'obligation de signaler soit conçue de manière à générer le moins de charge de travail possible et que la procédure de signalement permette de s'acquitter simultanément d'autres obligations de déclaration. Le projet crée les conditions juridiques nécessaires à la mise en place de ce type de solution.

Des participants ont également souhaité que l'obligation de signaler crée une plus-value pour les auteurs des signalements, ce qui renforcerait globalement l'économie. Une disposition a donc été ajoutée au projet afin de fixer explicitement le droit des exploitants d'infrastructures critiques – qui remplissent leur obligation de signaler – à un soutien de la part du NCSC.

Champ d'application de l'obligation de signaler

S'agissant du champ d'application personnel de l'obligation de signaler prévu à l'art. 74*b*, il a été relevé que le cercle des entités concernées était très vaste et devrait être précisé au niveau de l'ordonnance. Afin de pouvoir lever les doutes suffisamment tôt sur leur éventuel assujettissement à l'obligation de signaler, les intéressés peuvent s'informer à ce sujet auprès du NCSC. En cas de nécessité, ce dernier peut aussi rendre

des décisions relatives à l'assujettissement à l'obligation de signaler (art. 74*a*, al. 3, P-LSI). En outre, les critères d'exception à l'assujettissement à l'obligation de signaler ont été précisés (art. 74*c* P-LSI).

Il a également été demandé que l'obligation de signaler soit limitée aux parties d'entreprises qui exécutent des tâches visées à l'art. 74*b*, ceci étant particulièrement important pour les groupes qui déploient des activités dans des secteurs très diversifiés. De plus, lorsqu'une cyberattaque a des effets en Suisse, l'obligation de signaler devrait s'appliquer même si l'entreprise exploite ses moyens informatiques à l'étranger. Ces propositions ont été reprises dans deux nouveaux alinéas (art. 74*b*, al. 2 et 3, P-LSI).

Quant au champ d'application matériel, les participants à la procédure de consultation ont souhaité quelques précisions. La disposition qui définit les cyberattaques soumises à l'obligation de signaler (art. 74*d*) a donc été remaniée. Les critères qui n'étaient pas compréhensibles ou difficilement applicables ont été abandonnés. La disposition contenue à l'art. 74*a* de l'avant-projet, selon laquelle les cyberattaques devaient être signalées «le plus rapidement possible», a en outre été concrétisée et remplacée par un délai de signalement clairement mesurable de 24 heures (art. 74*e* P-LSI).

Confidentialité des signalements

Un autre point important aux yeux des participants à la procédure de consultation est que les signalements soient traités de manière confidentielle. Il a notamment été souhaité que les signalements au NCSC soient exclus du champ d'application de la LTrans. Dans le cas contraire, il existerait un risque que des informations sensibles des exploitants d'infrastructures critiques ayant signalé un cyberincident doivent être rendues publiques. Cette attente est satisfaite au moyen d'une exception au droit d'accès prévu par la LTrans pour les informations de tiers obtenues dans le cadre des signalements et de leur analyse (art. 4, al. 1bis, P-LSI).

Amende en cas de violation de l'obligation de signaler

La proposition qui a assurément soulevé le plus d'opposition est l'introduction d'une sanction en cas de non-respect de l'obligation de signaler. Avant de prononcer une sanction, le NCSC informe tout d'abord les intéressés de leur obligation de signaler, puis il exige le signalement de l'attaque au moyen d'une décision assortie d'une menace d'amende en cas de refus de se conformer à la décision. Une disposition supplémentaire a été ajoutée afin d'obliger le NCSC à informer les assujettis à l'obligation de signaler dès que toutes informations requises aux fins de l'obligation de signaler ont été fournies (art. 74*e*, al. 5, P-LSI). Cette procédure permet d'exclure des sanctions qui pourraient être dues à des ambiguïtés sur l'interprétation de l'obligation de signaler. Ce n'est que si l'assujetti à l'obligation de signaler ne remplit pas ses devoirs en dépit de la décision du NCSC, autrement dit s'il ne signale pas une cyberattaque concrète même a posteriori, qu'il est prévu de le sanctionner sous la forme d'une amende (art. 74*h* P-LSI).

Néanmoins, certains doutent qu'une amende soit le meilleur moyen pour faire appliquer l'obligation de signaler et 13 participants à la procédure de consultation exigent que l'article concerné soit biffé (art. 74*h* de l'avant-projet). Cette proposition n'a pas

été reprise. L'une des plus grandes avancées par rapport au système actuel des signalements à titre volontaire est que l'obligation de signaler va contraindre toutes les entités visées à échanger des informations et qu'il ne sera dès lors plus possible de profiter du système d'alerte précoce sans y contribuer. Si un assujetti refuse de participer activement à cet échange d'informations, il doit donc être possible de le sanctionner.

3 Comparaison avec le droit étranger, notamment européen

Depuis l'adoption, en juillet 2016, de la directive SRI[17], les membres de l'Union européenne sont tenus de mettre en œuvre une obligation de notifier les cyberincidents. Le délai pour ce faire était fixé à mai 2018. L'obligation concerne les «opérateurs de services essentiels», terme qui désigne, selon l'art. 4 de la directive SRI, les entreprises privées ou les entités publiques investies du rôle important d'assurer la sécurité dans les secteurs de la santé, des transports, de l'énergie, des banques et infrastructures de marchés financiers, des infrastructures numériques et de l'approvisionnement en eau. Le 16 mai 2022, le Parlement européen et la Commission européenne se sont mis d'accord sur une proposition de directive SRI révisée (SRI2) qui étend le champ d'application de l'obligation de notifier à huit nouveaux secteurs (traitement des eaux usées, gestion des déchets, administration publique, services postaux, alimentation, industrie, produits chimiques et navigation spatiale). Le cercle des entités visées par la directive SRI couvre donc largement celui des assujettis à l'obligation de signaler défini dans le présent projet.

En ce qui concerne l'étendue de l'obligation de notification, la directive SRI laisse une marge de manœuvre relativement importante aux États membres de l'UE. Les incidents graves doivent être déclarés, l'art. 14 précisant que l'appréciation de la gravité repose notamment sur le nombre d'utilisateurs touchés, la durée de l'incident de sécurité et sa portée géographique. Contrairement au présent projet, la directive SRI ne se limite toutefois pas à l'introduction d'une obligation de notification. Elle impose en même temps aux opérateurs de services essentiels de prendre des mesures de sécurité, par exemple pour prévenir les risques, pour garantir un niveau de sécurité adapté pour les réseaux et les systèmes d'information et pour limiter l'impact des incidents compromettant la sécurité (art. 14 de la directive SRI).

Le présent projet (P-LSI) se contente quant à lui de créer les bases légales nécessaires à de telles exigences dans le secteur de l'électricité. Dans les autres secteurs, il conviendra d'abord de déterminer si la Confédération a la compétence d'édicter des normes juridiquement contraignantes en matière de cybersécurité et quelles exigences devraient, le cas échéant, être imposées dans quels domaines.

17 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, JO L 194 du 19.7.2016, p. 1.

4 Présentation du projet

4.1 Réglementation proposée

L'introduction d'une obligation de signaler les cyberattaques contre des infrastructures critiques se justifie principalement par les possibilités d'alerte précoce et d'amélioration de la vue d'ensemble des menaces. Comme les auteurs de cyberattaques recourent souvent à des méthodes et à des schémas similaires pour plusieurs infrastructures critiques de différents secteurs, cette obligation peut renforcer considérablement la cybersécurité des infrastructures critiques en permettant d'identifier rapidement les méthodes d'attaque et en transmettant les alertes correspondantes. Vu le nombre élevé de signalements qui parviendront au NCSC en vertu de l'obligation de signaler, il sera possible d'évaluer la menace de façon plus précise.

Cette obligation ne s'applique qu'aux cyberattaques renfermant un potentiel de dommages important. Les cyberincidents relevant de l'erreur humaine, par exemple une manipulation fautive commise involontairement par un collaborateur, n'ont pas besoin d'être déclarés. Enfin, il a été décidé de ne pas étendre l'obligation de signaler aux vulnérabilités des équipements informatiques. Dans la plupart des cas, les vulnérabilités sont découvertes par des tiers (chercheurs en sécurité). Ceux-ci peuvent être motivés à communiquer les vulnérabilités au moyen d'incitations (par ex. par des programmes de type *bug bounty*, dits aussi de prime à la faille ou de prime au bogue) et une obligation de signaler pourrait plutôt avoir un effet dissuasif à cet égard.

Malgré l'introduction de l'obligation de signaler les cyberattaques, il reste possible de notifier les cyberincidents et les vulnérabilités à titre volontaire. Cette possibilité n'est pas réservée aux infrastructures critiques et est offerte à tout un chacun.

L'introduction de l'obligation de signaler les cyberattaques permet en même temps de régler au niveau de la loi les tâches du NCSC, qui ne sont actuellement définies que dans l'ordonnance du 27 mai 2020 sur les cyberrisques (OPCy)[18].

4.2 Adéquation des moyens requis

Le NCSC gère déjà à l'heure actuelle un service d'alerte qui recueille les signalements de cyberincidents effectués à titre volontaire. Il bénéficie en la matière de la longue expérience de MELANI, qui se chargeait de cette tâche depuis 2004.

Le NCSC utilise un formulaire électronique pour les signalements effectués à titre volontaire. Il est possible d'adapter ce système de signalement électronique afin qu'il puisse aussi servir à la réception des signalements découlant de l'obligation de signaler. Les coordinations nécessaires avec d'autres organes qui réceptionnent également des déclarations (par ex. PFPDT, Autorité fédérale de surveillance des marchés financiers [FINMA], Inspection fédérale de la sécurité nucléaire [IFSN]) et la configuration du formulaire de signalement requièrent un investissement initial qui peut néanmoins être couvert par les ressources existantes du NCSC. En vue de la mise en œuvre du projet, le NCSC doit toutefois pouvoir garantir la saisie correcte, la confirmation de la réception et la documentation des signalements effectués au titre de l'obligation de

18 RS **120.73**

signaler, ainsi que la transmission des informations sur la cybermenace qui en découlent aux organes ad hoc, aux fins de l'alerte précoce. Ce surcroît de travail devra être pris en compte lors des développements futurs du NCSC.

Après une cyberattaque, le NCSC apportera son soutien à l'infrastructure critique touchée pour l'aider à gérer l'incident. Cette prestation de soutien fonctionne déjà bien, grâce à la longue expérience du NCSC (et, auparavant, de celle de MELANI). Il faut cependant s'attendre à ce que l'introduction de l'obligation de signaler augmente la charge de travail du NCSC, parce que l'on peut s'attendre à ce que les signalements soient plus nombreux et que, en vertu de l'art. 74*a*, al. 3, le NCSC devra dorénavant procéder à une première évaluation et émettre les recommandations utiles pour régler l'incident. Il faudra dès lors étoffer encore son équipe chargée des analyses techniques (GovCERT).

4.3 Mise en œuvre

4.3.1 Nécessité d'une base légale

Il découle du principe de légalité (art. 5, al. 1, de la Constitution [Cst.][19]) et des dispositions relatives à la législation de l'art. 164, al. 1, Cst. que l'obligation de signaler les cyberattaques doit être réglée au moins dans les grandes lignes au niveau de la loi. Le projet contient par conséquent les éléments essentiels de l'obligation de signaler les cyberattaques: il comporte les principaux éléments de l'obligation de signaler, notamment ses facteurs déclenchants et sa portée (cyberattaques avec potentiel de dommages), le cercle des assujettis (exploitants d'infrastructures critiques actifs dans des domaines définis), le délai et le contenu du signalement ainsi que son utilisation par le NCSC. Pour les exploitants d'infrastructures critiques assujettis, l'obligation de signaler les cyberattaques constitue une atteinte à leurs droits de particuliers ou, si l'organisme responsable est cantonal ou communal, à leur autonomie fédéraliste. Cette atteinte est toutefois mineure et n'a pratiquement pas de conséquences financières pour les entreprises concernées.

4.3.2 La LSI, une base légale adéquate

Dans le cadre des travaux réalisés en amont de l'avant-projet, on a examiné si les nouvelles réglementations devaient être fixées dans une loi à part ou intégrées à un acte existant dont le but, l'objet et le champ d'application seraient compatibles avec une obligation de signaler les cyberattaques contre des infrastructures critiques[20]. Les actes législatifs contenant déjà des dispositions relatives aux infrastructures critiques et axés sur la protection de l'ordre public (LPPCi, loi du 17 juin 2016 sur l'approvisionnement économique du pays[21], loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure[22], LRens et LSI) ont notamment été

19 RS **101**
20 Cf. rapport du 25 novembre 2020 «Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen, Rechtliche Grundlagen», (disponible en allemand uniquement)
21 RS **531**
22 RS **120**

pris en considération pour servir de base à l'inscription dans la loi de l'obligation de signaler.

Après un examen approfondi, il est apparu que parmi ces actes, seule la LSI offrait un cadre adéquat. Son but, à savoir assurer la sécurité des informations traitées par la Confédération et des moyens informatiques qu'elle utilise, a un lien direct avec la cybersécurité (bien que la loi n'utilise pas ce terme). En outre, certains articles de la LSI prévoient déjà le soutien des infrastructures critiques par la Confédération, et donc une partie du mandat du NCSC. Par conséquent, la LSI n'était pas seulement adéquate, mais elle représentait même une base légale idéale pour inscrire dans la loi l'obligation de signaler les cyberattaques. De plus, l'introduction d'une obligation, pour les exploitants d'infrastructures critiques, de signaler les «incidents graves» avait été discutée lors des débats parlementaires sur le projet de loi, mais elle avait été rejetée par la majorité du Conseil national en juin 2020, après que le Conseil fédéral avait indiqué qu'un projet de loi serait élaboré à cet effet.

4.3.3 Dispositions d'exécution

La mise en œuvre de l'obligation de signaler incombe au NCSC. Le Conseil fédéral a d'ores et déjà décidé, le 12 mai 2022, que ce dernier serait transformé en office fédéral. Le NCSC disposera ainsi des bases d'organisation nécessaires pour pouvoir assumer les tâches qui lui sont confiées par le projet.

Le Conseil fédéral concrétisera les dispositions légales relatives aux tâches du NCSC et à l'obligation de signaler les cyberattaques dans une ordonnance. En vertu de l'art. 182, al. 2, Cst., le Conseil fédéral peut édicter des dispositions d'exécution, soit des normes secondaires, pour tous les articles du chapitre 5. Une norme de délégation n'est pas nécessaire puisqu'aucune compétence normative ne lui est déléguée, excepté la compétence de mettre la loi en vigueur. Il peut donc décider librement quelles dispositions de la loi il convient de préciser dans une ordonnance. Le Conseil fédéral est toutefois tenu de définir les seuils applicables pour les exceptions prévues à l'obligation de signaler prévues à l'art. 74*c*, en tenant compte des critères indiqués dans cette disposition.

4.3.4 Applicabilité de l'obligation de signaler

Les avis exprimés lors de la procédure de consultation montrent clairement que l'obligation de signaler est largement soutenue, pour autant que le signalement n'occasionne qu'une faible charge de travail pour les assujettis et que cela leur apporte une plus-value sur le plan de la cybersécurité. Pour que les assujettis puissent satisfaire à leur obligation de signaler, un formulaire en ligne sera développé afin qu'il soit possible de saisir rapidement les données requises puis de les transmettre électroniquement au NCSC. Le NCSC dispose déjà d'une certaine expérience dans la mise en place de portails de signalement puisque, depuis 2020, la population et les entreprises peuvent lui transmettre des signalements à titre volontaire. Il veillera à ce que les procédures de signalement soient aussi simples que possible et cherchera un contact direct à ce sujet avec les assujettis à l'obligation de signaler.

Outre l'obligation d'informer le NCSC, une cyberattaque contre une infrastructure critique peut affecter d'autres processus soumis à une obligation de signaler, et donc

engendrer simultanément plusieurs obligations. On peut par exemple se trouver en présence des chevauchements suivants:

– Pour les infrastructures critiques du secteur financier soumises à la surveillance de la FINMA, une obligation de signaler les cyberattaques à cette autorité[23] est en vigueur depuis le 1er septembre 2020 déjà.

– Une cyberattaque contre une infrastructure critique peut entraîner une violation de la sécurité des données qui, en fonction de sa gravité, doit être annoncée au PFPDT (art. 24 nLPD).

– Si une cyberattaque provoque des dysfonctionnements au sein de l'infrastructure critique, par ex. un incident radioactif dans une centrale nucléaire, celui-ci doit généralement aussi être déclaré (IFSN, Centrale nationale d'alarme, etc.).

La nouvelle obligation de signaler les cyberattaques ne remplacera pas les obligations de déclaration existantes, qui demeurent inchangées. Il est donc important que la charge de travail soit acceptable pour les assujettis à l'obligation de signaler s'ils doivent en même temps s'acquitter d'autres obligations de déclaration. Voilà pourquoi le NCSC mettra à disposition un système permettant la saisie électronique du signalement (formulaire, masque ou autre), que les assujettis à l'obligation de signaler pourront utiliser pour transmettre des informations à d'autres guichets de signalement, pour autant que ces derniers collaborent. Le NCSC contribue ainsi à exploiter les synergies entre les obligations de déclaration existantes, si ces dernières présentent un lien avec la cyberattaque ou ses effets.

Les assujettis à l'obligation de signaler pourront décider eux-mêmes si le signalement saisi électroniquement auprès du NCSC doit être transmis à d'autres organes et, le cas échéant, s'il doit l'être en tout ou en partie, voire avec des informations complémentaires. L'important est que les données spécifiques nécessaires à l'exécution de chacune des obligations de déclaration ne soient accessibles que pour l'organe concerné. Les assujettis à l'obligation de signaler pourront déterminer lors de la saisie et de la transmission quelles informations sont envoyées à quel guichet de signalement.

5 Commentaire des dispositions

5.1 Considérations générales

Les bases légales de l'obligation de signaler les cyberattaques sont intégrées au chapitre 5 de la LSI, ce à quoi il faut ajouter la modification du titre de l'acte et quelques adaptations mineures au chapitre 1. Le chapitre 5 a subi un remaniement de fond pour qu'il puisse aussi définir les tâches du NCSC, qui ne concernent pas uniquement

23 Cf. communication FINMA sur la surveillance nº 05/2020 du 7 mai 2020, qui se fonde sur l'art. 29, al. 2, de la loi sur la surveillance des marchés financiers (RS **956.1**).

l'obligation de signaler et ne sont pas spécifiquement axées sur les infrastructures critiques. Le titre de ce chapitre est donc modifié («Chapitre 5 Mesures de la Confédération afin de protéger la Suisse contre les cybermenaces»).

Les principales règles contenues dans les dispositions légales ont déjà été décrites et motivées – pour certaines de manière détaillée – sous les chiffres précédents. Les commentaires relatifs aux articles se limitent donc à des compléments d'information. S'agissant des dispositions qui ne subissent que des changements formels, les explications fournies dans le message du 22 février 2017 concernant la loi sur la sécurité de l'information[24] demeurent valables.

5.2 Commentaire article par article

Titre

Le titre «loi fédérale sur la sécurité de l'information au sein de la Confédération» devient «loi fédérale sur la sécurité de l'information». Si les dispositions sur la sécurité de l'information concernent principalement la Confédération, celles sur la cybersécurité de la Suisse, qui est définie comme une tâche du NCSC et fait l'objet du chapitre 5, ne concernent pas uniquement la Confédération. La nouvelle obligation de signaler les cyberattaques s'applique sur l'ensemble du territoire national et vise également les autorités cantonales et les organisations intercantonales.

Chapitre 1 Dispositions générales

Dans le premier chapitre, seuls les art. 1, 2, 4 et 5 sont modifiés. Les autres articles ne changent pas.

Art. 1 But

L'al. 1 de l'article définissant le but de la LSI a été complété et subdivisé en deux lettres a et b. La let. a reprend la formulation d'origine, tandis que la let. b vient fixer en complément l'objectif en matière de cybermenaces. L'extension de la finalité de la loi permet de prendre en considération les nouveaux éléments qui accompagnent l'introduction de l'obligation de signaler les cyberattaques et de la réglementation légale des tâches du NCSC.

Art. 2 Autorités et organisations concernées

Dans l'al. 5, le renvoi aux dispositions qui s'appliquent aux infrastructures critiques a été adapté, puisque le chapitre 5 commence désormais par l'art. 73*a* et se termine par l'art. 79. Cet article n'a par contre subi aucune modification de fond.

Art. 4 Rapport avec d'autres lois fédérales

Lors de la procédure de consultation concernant l'avant-projet, plusieurs participants ont relevé que la confidentialité des signalements adressés au NCSC devait être garantie et qu'il convenait donc d'exclure le NCSC du champ d'application de la LTrans.

Cette proposition est reprise en partie avec l'ajout d'un al. 1bis à l'art. 4 LSI, qui règle les rapports avec la LTrans. Ce nouvel alinéa exclut que les informations de tiers dont

24 FF **2017 2765** p. 2872 ss

le NCSC prend connaissance dans le cadre de sa fonction de guichet de signalement, que ce soit en relation avec des signalements ou avec leur analyse, soient rendues accessibles. Le législateur a toutefois renoncé à exclure entièrement le NCSC du champ d'application de la LTrans.

Il faut que le NCSC puisse garantir aux auteurs des signalements que leurs signalements seront traités de manière confidentielle. Cette relation de confiance est une condition essentielle pour que les infrastructures critiques s'acquittent de la nouvelle obligation de signaler les cyberattaques. La garantie de la confidentialité gagne en importance avec la création de l'obligation de signaler, car cela va entraîner une augmentation du nombre de signalements traités par le NCSC.

Depuis l'adoption de l'OPCy (en mai 2020) et de la version initiale de la LSI (en décembre 2020), le champ d'activité du NCSC s'est élargi, notamment en raison de l'obligation de signaler.

Pour permettre au NCSC d'exécuter les tâches qui lui incombent dans sa fonction de guichet de signalement et compte tenu de l'augmentation du nombre de signalements, il est indispensable de soustraire les informations de tiers dont le NCSC prend connaissance en relation avec les signalements et leur analyse du droit d'accès prévu par la LTrans. En revanche, les informations émanant d'autorités et d'organisations qui sont elles-mêmes assujetties à la LTrans restent soumises au droit d'accès conformément à la LTrans.

Une exception est par ailleurs prévue pour l'obligation de signaler les cyberincidents dans le secteur financier, la fonction de guichet de signalement étant ici revêtue par l'autorité de surveillance qu'est la FINMA. Contrairement au NCSC, la FINMA est entièrement exclue du champ d'application de la LTrans (art. 2, al. 2, LTrans). S'agissant du NCSC, seul est exclu le droit d'accès aux informations de tiers portées à sa connaissance dans l'exercice de sa fonction de guichet de signalement. Pour le reste, la LTrans continue de primer la LSI (art. 4, al. 1, LSI).

Art. 5 Définitions

Les définitions des let. a, b et c ne sont pas modifiées. En rapport avec l'obligation de signaler des cyberattaques prévue à l'art. 74*a* ss, il convient de relever que les infrastructures critiques sont définies de manière ouverte à la let. c. Cette définition ne peut donc pas être utilisée comme base directe pour définir le cercle des assujettis à l'obligation de signaler.

Quatre nouvelles notions sont ajoutées à la liste des termes définis (d. cyberincident, e. cyberattaque, f. cybermenace et g. vulnérabilité). Ces termes ont une portée immédiate pour la nouvelle obligation de signaler, raison pour laquelle il est nécessaire d'en donner une définition légale. Les nouvelles définitions introduites dans cet article correspondent aux définitions utilisées dans les normes internationales reconnues[25].

25 En particulier, ISO 27000; ISO/IEC 29147:2018; NIST.

Let. d: cyberincident

La définition du cyberincident montre clairement qu'il s'agit d'un terme générique qui recouvre tous les événements qui pourraient porter atteinte aux objectifs de protection des informations visés à l'art. 6, al. 2, LSI, à savoir la confidentialité, la disponibilité et l'intégrité des informations ainsi que la traçabilité de leur traitement. L'intégrité des informations est garantie lorsque leur incorruptibilité et leur exactitude sont assurées. La traçabilité du traitement consiste à ce que l'on puisse déterminer par qui, quand et de quelle manière les informations ont été traitées (cf. explications données dans le message du 22 février 2017 concernant la loi sur la sécurité de l'information) [26].

Un cyberincident peut aussi bien être un événement provoqué intentionnellement par un tiers non autorisé (cyberattaque) qu'un événement causé involontairement par une personne autorisée (par ex. par une fausse manipulation) ou encore un événement dû à un dysfonctionnement des moyens informatiques. Cette dernière catégorie inclut également les erreurs des systèmes de décision algorithmiques (intelligence artificielle, AI).

L'aspect essentiel d'un cyberincident est l'atteinte à la confidentialité, à la disponibilité ou à l'intégrité d'informations [27] ou à la traçabilité de leur traitement. Les événements qui auraient le potentiel de porter atteinte aux objectifs de protection, mais qui ne les affectent pas concrètement, ne sont pas des cyberincidents au sens de la présente loi, mais seulement des cybermenaces au sens de la let. f. Cette restriction et cette distinction sont nécessaires, car les organisations et les entreprises sont confrontées quotidiennement à un grand nombre d'événements qui portent théoriquement atteinte aux objectifs de protection, mais qui, dans les faits, peuvent être déjoués grâce aux mesures de protection techniques mises en place (on parle ici de tentatives d'hameçonnage, de pourriels, etc.). C'est donc uniquement en cas d'atteinte effective aux objectifs de protection que l'événement peut être qualifié de cyberincident.

Let. e: cyberattaque

La cyberattaque est l'une des formes possibles du cyberincident. Un cyberincident est qualifié de cyberattaque lorsqu'il est provoqué intentionnellement, indépendamment de savoir s'il s'agit de collaborateurs internes ou d'une source externe (voire des deux). L'aspect déterminant n'est pas le lieu d'origine de l'attaque (interne ou externe), mais le fait que l'auteur de l'attaque a intentionnellement porté atteinte aux objectifs de protection, à savoir la confidentialité, la disponibilité et l'intégrité des informations ainsi que la traçabilité de leur traitement (cf. définition du cyberincident à la let. d). La manière dont la cyberattaque est définie implique que seules les attaques réussies sont qualifiées de cyberattaques, autrement dit celles qui n'ont pas pu être – entièrement – déjouées.

La distinction entre les cyberattaques et les cyberincidents est importante, parce que des cyberattaques peuvent se reproduire plusieurs fois selon le même schéma. Avoir

26 FF **2017** 2765 p. 2828

27 Le terme «informations» est utilisé dans la LSI comme un terme générique qui inclut également les données personnelles.

une vue d'ensemble des modes opératoires est donc essentiel pour être en mesure d'avertir de manière précoce les infrastructures critiques.

C'est pour cette raison que l'obligation de signaler est limitée aux cyberattaques, tandis que les autres cyberincidents (par ex. ceux provoqués involontairement par des fausses manipulations effectuées par des collaborateurs) et les cybermenaces (par ex. les tentatives d'attaques infructueuses ou les vulnérabilités) peuvent toujours être signalés à titre volontaire et par toute personne. Les cyberattaques doivent être signalées dès lors qu'elles touchent des sous-secteurs critiques (art. 74*b*) et qu'elles ont un certain degré de gravité (art. 74*d*).

Let. f: cybermenace

On entend par cybermenace toute circonstance ou tout événement pouvant entraîner un cyberincident. Cette définition englobe donc aussi tous les événements déjoués avec succès, comme les tentatives d'hameçonnage. Cette définition se fonde sur la définition internationalement reconnue de la notion de *cyberthreat*[28].

La notion de cybermenace doit être privilégiée par rapport à celle de cyberrisque, couramment utilisée jusqu'à présent. Au sens strict, un cyberrisque n'est pas une cybermenace, mais une simple appréciation de la probabilité qu'une menace se concrétise et de l'ampleur des dommages qui peuvent en découler.

Let. g: vulnérabilité

La notion de vulnérabilité, soit une cybermenace due à des failles ou à des erreurs dans les moyens informatiques, est elle aussi ajoutée à la liste des définitions légales. Une vulnérabilité est une forme de cybermenace.

La définition choisie s'inspire de celle du terme *vulnerability* donnée par le National Institute of Standards and Technology aux États-Unis[29]. Une vulnérabilité peut trouver son origine dans la conception, l'implémentation, la configuration ou l'exploitation des moyens informatiques, dans les algorithmes utilisés ou dans l'organisation. Certaines définitions de la vulnérabilité (*vulnerability*) opèrent une distinction en fonction du degré de vulnérabilité (*degree of vulnerability*)[30]. Dans le cas présent, la définition de divers degrés de vulnérabilité n'a pas été jugée nécessaire.

Une vulnérabilité peut elle-même être à l'origine d'un cyberincident, par exemple lorsque des dysfonctionnements entraînent un cryptage des données insuffisant, avec une mise en péril immédiate de la confidentialité des données. Mais dans la plupart

28 NIST: Cyber Threat - Glossary | CSRC (nist.gov); ISO: ISO/IEC TS 27100:2020(en), Information technology — Cybersecurity — Overview and concepts; ENISA: Glossary — ENISA (europa.eu).

29 Sur son site, le National Institute of Standards and Technology (NIST) du Département américain du commerce donne la définition suivante: «Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.» Dans le glossaire CISA de la National Initiative for Cybersecurity Careers and Studies (NICCS), il apparaît clairement qu'une *weakness* est un stade préliminaire qui précède une *vulnerability*.

30 Cf. glossaire CISA: «Vulnerability (expressing degree of vulnerability): qualitative or quantitative expression of the level of susceptibility to harm when a threat or hazard is realized»

des cas, une vulnérabilité des moyens informatiques se traduit seulement par une plus grande exposition à des cyberincidents, en servant par exemple de porte d'entrée pour des cyberattaques.[31].

Chapitre 2 Mesures générales

Section 1: Principes

Un nouvel art. 10*a*, sans aucun rapport avec la mise en place de l'obligation de signaler ou avec les tâches légales du NCSC, est ajouté à la fin de la section 1 du chapitre 2. Il convient en effet de profiter de la révision partielle relative à l'obligation de signaler pour inscrire cette disposition dans la LSI afin de remédier à une lacune, à savoir l'absence de disposition légale matérielle en rapport avec le traitement de données personnelles dans le contexte de la sécurité de l'information.

Art. 10a Traitement des données personnelles

Dans le cadre de la gestion de la sécurité de l'information, par exemple pour la formation ou les audits, des données personnelles sont régulièrement traitées. Pour le traitement de ces données, une base juridique au niveau de l'ordonnance est généralement suffisante. En revanche, la gestion d'incidents de sécurité suppose le traitement de données portant sur les auteurs potentiels d'infractions qui peuvent être liées à des poursuites et des sanctions administratives ou pénales et qui sont donc considérées comme des données sensibles au sens de l'art. 3, let. c, de la loi fédérale du 19 juin 1992 sur la protection des données (LPD).[32] en vigueur et de l'art. 5, let. c, nLPD. La nLPD sera déjà applicable lorsque le présent projet entrera lui-même en vigueur, raison pour laquelle l'art. 10*a* renvoie déjà à celle-ci.

La loi sur la protection des données exige, pour le traitement de données sensibles, une base légale, qui faisait défaut jusqu'ici et qui est désormais créée avec l'art. 10*a*. Les données sensibles sont notamment les informations sur l'identité, les activités, la manière d'agir et les motivations des auteurs potentiels d'infractions. Font également l'objet d'un traitement les données des personnes susceptibles d'être affectées par un incident, par exemple parce qu'elles subissent un dommage.

Pour le traitement des données personnelles conformément à la LPD, le principe de proportionnalité doit être respecté, raison pour laquelle les données sensibles ne peuvent être conservées que pendant deux ans après la résolution des violations de la sécurité de l'information ou l'élimination des vulnérabilités. Le délai maximal pour le traitement des données sensibles est de 10 ans, puisqu'aucune procédure définie n'est prévue par la loi, comme c'est le cas par exemple pour le code de procédure pénale.

L'art. 10*a* ne porte pas sur le traitement des données personnelles par le NCSC. Cet aspect est réglé aux art. 75 ss.

31 Cf. la définition de *vulnerability* dans NISTIR 7511 Rev. 4: «error, flaw, or mistake in computer software that permits or causes an unintended behavior to occur»

32 RS **235.1**

Art. 23 Zones de sécurité

Al. 3

Modifications rédactionnelles dans le texte français.

Chapitre 3 Contrôle de sécurité relatif aux personnes

Art. 44 Voies de droit

Al. 2

Modifications rédactionnelles.

Chapitre 5 Mesures de la Confédération afin de protéger la Suisse contre les cybermenaces

Aucune modification n'a été apportée au chapitre 4.

Le chapitre 5, en revanche, voit l'introduction de l'obligation de signaler les cyberattaques contre les infrastructures critiques et de dispositions fondamentales concernant les tâches du NCSC. Pour garantir une meilleure vue d'ensemble, le chapitre 5 est désormais divisé en trois sections: «Section 1 Dispositions générales», «Section 2 Obligation de signaler les cyberattaques» et «Section 3 Protection des données et échange d'informations».

Section 1: Dispositions générales

Les dispositions de la section 1 énoncent des principes généraux concernant, par exemple, la procédure de signalement et la façon dont les signalements sont traités par le NCSC, et qui sont aussi applicables à l'obligation de signaler (section 2) ainsi qu'à la protection des données et à l'échange d'informations (section 3).

Art. 73a Principe

Al. 1

L'al. 1 décrit l'activité d'analyse du NCSC comme la condition préalable à l'accomplissement de ses tâches. Les analyses techniques du NCSC comprennent aussi la recherche à large échelle de sites Internet infectés ou de vulnérabilités.

Al. 2

Les let. a à e de l'al. 2 décrivent les tâches du NCSC. Il s'agit d'une liste non exhaustive. Les différentes tâches ainsi que la collaboration avec les autorités en Suisse et à l'étranger sont concrétisées dans d'autres articles et seront commentées à cet endroit.

Art. 73b Signalements

Depuis le 1er janvier 2020, le NCSC exploite un guichet unique suisse en matière de cyberrisques (art. 12, al. 1, let. a, OPCy), qui enregistre et traite les signalements de cyberincidents et de cybermenaces. Le guichet de signalement du NCSC a été développé à partir de MELANI, qui réceptionnait les déclarations depuis 2004. Il est utilisé activement par les entreprises et la population: en 2021, il a reçu 21 714 signalements.

Al. 1

Dans sa fonction de guichet de signalement, le NCSC reçoit les signalements volontaires de cyberincidents et de cybermenaces, mais aussi les signalements des cyberattaques visées par l'obligation de signaler. Ce deuxième aspect n'est pas mentionné explicitement dans la loi, puisque les cyberattaques sont une forme de cyberincident.

Les cyberincidents et les cybermenaces, en particulier les vulnérabilités, peuvent être signalés par des tiers et pas uniquement par les victimes elles-mêmes, et ce, également de manière anonyme. Les auteurs de signalements doivent s'assurer qu'ils sont autorisés à le faire, surtout s'ils agissent pour le compte de tiers. L'al. 1 n'est donc pas une norme d'autorisation qui permettrait de dédouaner les lanceurs d'alerte. Les obligations de garder le secret contractuelles ou légales doivent être respectées.

La découverte de vulnérabilités par le biais d'un accès non autorisé aux moyens informatiques de tiers (piratage)[33] reste donc punissable. Il n'est pas judicieux de créer un régime de protection (*legal safe harbour*) pour les chercheurs en sécurité qui signalent des vulnérabilités, car les pirates «criminels» resteraient eux aussi impunis ou pourraient à tout le moins éviter d'être poursuivis en effectuant un signalement. Le piratage informatique reste donc punissable. Mais, en vertu de l'art. 73*d*, al. 3, le personnel du NCSC n'est pas soumis à l'obligation de dénoncer prévue à l'art. 22*a* LPers. De plus, les pirates ou les chercheurs en sécurité peuvent signaler de manière anonyme les vulnérabilités qu'ils découvrent.

Al. 2

Le NCSC analyse les signalements et évalue leur importance pour la protection de la Suisse contre les cybermenaces. Si les signalements ne sont pas anonymes et que leurs auteurs le souhaitent, le NCSC peut donner son avis sur l'incident en se basant sur ses analyses et émettre des recommandations quant aux mesures à prendre.

Le NCSC traite les signalements en toute confidentialité. C'est une condition essentielle pour que les signalements soient faits et que le guichet de signalement jouisse de la confiance des entreprises. Pour cette raison, le personnel du NCSC est exempté de l'obligation de dénoncer les infractions (art. 73*d*, al. 3) et les informations portées à la connaissance du NCSC dans sa fonction de guichet de signalement sont soustraites au droit d'accès prévu par la LTrans (art. 4, al. 1bis).

Al. 3

Les vulnérabilités augmentent l'exposition des moyens informatiques aux cyberincidents et représentent une cybermenace (art. 5, let. f et g). Les vulnérabilités peuvent être signalées au NCSC sur une base volontaire. Il n'existe aucune obligation de signaler à cet égard.

Lorsqu'une vulnérabilité lui est signalée, le NCSC en informe le fabricant du logiciel ou du matériel informatique concerné selon la procédure dite de divulgation coordonnée des vulnérabilités (*coordinated vulnerability disclosure*[34]), afin que celui-ci puisse éliminer la vulnérabilité et proposer une solution à ses utilisateurs, par exemple

33 Cf. l'infraction de piratage informatique à l'art. 143bis CP (RS **311.0**).
34 L'expression *responsible vulnerability disclosure* est également utilisée.

un correctif (*fix* ou *patch*). Le mot «fabricant» doit être pris dans son acception fonctionnelle et inclut donc aussi, par exemple, les développeurs de logiciels.

Le NCSC impartit au fabricant un délai pour éliminer la vulnérabilité, en l'informant que tout manquement pourra conduire à l'exclusion des procédures d'adjudication ou à la révocation d'adjudications[35], et que le NCSC pourra rendre publique la vulnérabilité à l'expiration du délai.

Lorsque le fabricant propose une solution pour éliminer une vulnérabilité, mais qu'il ne l'intègre pas lui-même au produit, il appartient aux utilisateurs de décider s'ils optent pour cette solution ou non. Une obligation d'éliminer les vulnérabilités serait une atteinte lourde à la liberté économique, et le contrôle de son exécution nécessiterait des moyens considérables. Du point de vue technique, il n'est d'ailleurs pas pertinent d'effectuer une mise à jour de sécurité de tous les systèmes dans tous les cas de figure. C'est la raison pour laquelle le Conseil fédéral a renoncé à introduire des obligations à cet égard.

Art. 73c Publication d'informations provenant de signalements

Al. 1

Le NCSC peut publier des informations sur des cyberincidents, à condition que ces informations ne contiennent pas de données concernant des personnes physiques ou morales. Ces informations ne doivent permettre de connaître l'identité de la personne physique ou morale concernée que si celle-ci y consent et que les caractères d'identification et les ressources d'adressage ont été utilisés de manière abusive, comme dans le cas de l'utilisation abusive d'un logo lors d'une attaque de type hameçonnage. En cas d'utilisation abusive de caractères d'identification, les lésés ne sont généralement pas que les organisations ou autorités propriétaires du logo, mais également des particuliers (par ex. des clients). Le cas échéant, le NCSC sollicitera le consentement de l'organisation ou de l'autorité dont le logo a été utilisé de manière abusive afin de pouvoir informer le public de l'abus.

Al. 2

La publication rapide d'une vulnérabilité avec l'indication du logiciel ou du matériel informatique concerné peut s'avérer nécessaire pour prévenir d'autres cyberattaques. En septembre 2021, le NCSC a été reconnu par l'organisation américaine MITRE comme organe habilité à attribuer des numéros d'identification uniques aux vulnérabilités, qui sont qualifiées dans ce contexte de *common vulnerabilities and exposures* (CVE). Les numéros CVE sont attribués selon un système de référence international et servent à identifier, à définir et à cataloguer les vulnérabilités rendues publiques dans le cadre de la cybersécurité.

Les vulnérabilités sont rendues publiques conformément à la procédure de divulgation coordonnée des vulnérabilités, qui est actuellement considérée comme une bonne pratique et est également appliquée par les programmes de prime à la faille (*bug bounty*).

35 Cf. l'ajout proposé à l'art. 44, al. 1, let. f^{bis}, LMP dans le cadre du présent projet de révision de la LSI.

Le fabricant dispose d'un certain temps pour éliminer la vulnérabilité avant sa publication et le NCSC lui impartit un délai concret à cette fin.

Souvent, la publication d'une vulnérabilité n'a plus de raison d'être si le fabricant l'a éliminée, en particulier lorsqu'il le fait au moyen d'un correctif automatique. Mais dans certains cas, il peut tout de même s'avérer judicieux d'attirer l'attention du public sur une vulnérabilité, même si le fabricant l'a déjà éliminée. Dans ce cas, la publication ne peut se faire qu'avec le consentement du fabricant. Si le fabricant n'élimine pas la vulnérabilité, le NCSC peut la publier sans son consentement. Le NCSC renonce à la publication si cela ne sert pas la protection contre les cybermenaces, par exemple si la publication aurait pour effet d'informer les auteurs d'attaques sur des vecteurs possibles avant qu'ils ne les aient découverts par leurs propres moyens (*zero day exploits*).

L'al. 2 crée la base légale qui permet au NCSC d'indiquer le nom du matériel informatique ou du logiciel concerné et donc, implicitement, celui de leur fabricant lorsque ce dernier n'élimine pas la vulnérabilité dans le délai imparti.

Art. 73d Transmission d'informations

L'art. 73*d* définit les conditions auxquelles le NCSC est autorisé à transmettre à d'autres autorités et organisations des informations pertinentes en matière de sécurité provenant d'un signalement ou de son analyse (al. 1 à 3).

Si ces informations contiennent des secrets protégés par la loi ou par contrat, le collaborateur du NCSC responsable de la transmission doit être délié de son secret de fonction selon la procédure prévue à l'art. 320 du Code pénal (CP).[36] afin de ne pas être punissable (al. 4).

Al. 1

Les conditions posées pour la transmission d'informations aux autorités et aux organisations actives dans le domaine de la cybersécurité sont cumulatives. La transmission ne peut donc se faire que si les informations en question sont utiles aux spécialistes en cybersécurité auxquels elles sont destinées dans le cadre de la protection contre les cybermenaces et, pour autant que ces informations permettent de connaître l'identité de la personne physique ou morale concernée, que si cette dernière a donné son consentement à la transmission.

La transmission aux spécialistes en cybersécurité ne nécessite pas qu'il y ait eu une usurpation d'identité, contrairement à ce qui est exigé pour la publication des mêmes informations en vertu de l'art. 73*c*, al. 1.

Al. 2

Le mandat du SRC consiste à déceler à temps et à prévenir les menaces pour la sûreté intérieure ou extérieure, à apprécier la menace et à alerter les infrastructures critiques sur les menaces (art. 6, al. 1, let. a, 2 et 5 LRens). Les informations provenant des signalements de cyberattaques et de leur analyse par le NCSC peuvent être pertinentes dans le cadre de l'accomplissement de ces tâches. C'est la raison pour laquelle le

36 RS **311.0**

NCSC transmet au SRC les informations qui lui sont nécessaires en vue de l'accomplissement de ses tâches. La transmission d'informations au SRC concerne uniquement les informations liées aux signalement de cyberincidents et à leur analyse, et non les informations sur les vulnérabilités signalées.

Al. 3

L'obligation de dénoncer à laquelle est soumis le personnel de la Confédération (art. 22*a* LPers) ne vaut pour les collaborateurs du NCSC que vis-à-vis du directeur de cette entité lorsque, dans le cadre d'un signalement ou de son analyse, ils obtiennent des informations sur une éventuelle infraction grave. Cette exception est nécessaire, car l'obligation de dénoncer est en contradiction avec le principe de la confidentialité du traitement des signalements par le NCSC. Il va néanmoins de soi que les collaborateurs du NCSC restent soumis à cette obligation s'ils découvrent les indices d'une infraction en dehors de la procédure de signalement et d'analyse.

Le directeur du NCSC peut se tourner vers les autorités de poursuite pénale lorsqu'il a un soupçon d'infraction grave fondé sur des informations provenant de signalements ou de leur analyse. Le NCSC n'effectue toutefois aucun acte d'instruction.

Ce droit de dénoncer pour les cas exceptionnels a été prévu pour les cas où l'analyse d'un incident déboucherait, par exemple, sur la découverte de matériel pédopornographique. Avant de dénoncer l'infraction, le directeur du NCSC doit peser les intérêts de l'État à une poursuite pénale et celui de l'auteur du signalement à la confidentialité des informations.

La problématique de l'auto-incrimination de l'auteur d'un signalement est réglée dans le cadre de l'obligation de signaler. Au lieu d'une interdiction d'obliger une personne à s'auto-incriminer telle qu'elle est prévue dans le droit de la protection des données (art. 24, al. 6, nLPD), la loi fixe ici que l'assujetti ne saurait s'auto-incriminer dans le but d'exécuter son obligation de signaler (cf. explications données au sujet de l'art. 74*e*, al. 4).

Al. 4

Dans les cas exceptionnels où une transmission d'informations au SRC ou aux autorités de poursuite pénale est envisageable en vertu des al. 2 et 3, les collaborateurs du NCSC responsables de la transmission doivent d'abord être déliés du secret de fonction conformément aux prescriptions de l'art. 320 CP, si les informations contiennent des secrets protégés par le droit pénal.

Art. 74 Soutien aux exploitants d'infrastructures critiques

Dans l'énumération non exhaustive des tâches du NCSC donnée à l'art. 73*a* figure, outre la réception et le traitement des signalements (cf. art. 73*b* à 73*d*), le soutien aux exploitants d'infrastructures critiques (let. e). L'étendue de ce soutien est concrétisée à l'art. 74.

La définition des infrastructures critiques visée à l'art. 5, let. c, LSI étant très large, il règne un certain flottement quand il s'agit de déterminer si une entreprise ou une organisation doit être considérée comme une infrastructure critique ou non.

De plus, les infrastructures critiques visées à l'art. 2, al. 1 à 3, LSI (comme les autorités fédérales) sont soumises à d'autres dispositions de la LSI qui ne s'appliquent pas à des infrastructures critiques comme la Migros.

Al. 1 et 2

Le NCSC soutient les exploitants d'infrastructures critiques dans la protection contre les cybermenaces. À cette fin, il met à leur disposition différents outils à titre gratuit. Les exploitants d'infrastructures critiques sont entièrement libres de profiter du soutien du NCSC ou pas. Les outils proposés peuvent être utilisés librement.

Les principaux outils sont énumérés à titre d'exemples (let. a à c). Il s'agit d'une liste non exhaustive.

Let. a

L'échange d'informations est un moyen essentiel pour protéger les infrastructures critiques contre les cybermenaces. La rapidité avec laquelle la situation en matière de menace évolue et la nécessité de prendre des mesures de protection requièrent des responsables qu'ils disposent constamment des informations les plus actuelles. Échanger avec les autres responsables est le moyen le plus efficace d'y parvenir. Le NCSC poursuit une collaboration qui a fait ses preuves via MELANI en mettant à la disposition des exploitants d'infrastructures critiques une plateforme destinée à cet échange d'informations. Le NCSC utilise aussi ce canal d'information sécurisé pour informer précocement les infrastructures critiques des modes opératoires qui n'ont pas encore été rendus publics ou que le NCSC ne peut pas publier pour des raisons de sécurité.

Let. b

Le NCSC met à la disposition des exploitants d'infrastructures critiques des informations techniques sur les cybermenaces actuelles (comme des vulnérabilités) et des recommandations sur les mesures préventives et réactives à mettre en place contre les cyberincidents. Les outils mentionnés à la let. b se limitent aux éléments susceptibles d'être utiles aux infrastructures critiques en général. Le NCSC ne fournit pas de conseils personnalisés aux infrastructures critiques.

Let. c

Des instruments techniques et des instructions pour la détection précoce des cyberincidents sont un autre soutien proposé par le NCSC. Ces instruments sont, par exemple, des règles de détection permettant d'identifier les flux de réseaux et les fichiers potentiellement nuisibles, des listes d'indicateurs techniques sur les attaques ou les tentatives d'attaques (*indicators of compromise*) ou des applications spécialisées servant à découvrir les modes opératoires et à se protéger contre ces attaques.

Certains de ces outils sont conçus de manière à être utiles à toutes les infrastructures critiques. Mais ils peuvent aussi être spécifiquement élaborés pour certains groupes d'infrastructures critiques ou pour certains domaines d'activité. Ils ne remplacent pas les dispositifs de protection individuels des infrastructures, mais peuvent y être intégrés.

Al. 3

Le NCSC peut venir en aide aux exploitants d'infrastructures critiques dans la gestion des cyberincidents et l'élimination des vulnérabilités en leur prodiguant des conseils techniques. Le soutien du NCSC est fourni sur demande et en étroite collaboration avec les infrastructures critiques concernées.

Le NCSC peut en outre fournir une assistance technique aux exploitants d'infrastructures critiques lorsque des cyberincidents mettent en péril le fonctionnement de l'infrastructure concernée. Le soutien technique du NCSC constitue une mesure d'urgence. Les mesures plus étendues, notamment celles visant à rétablir la cybersécurité en général, sont du ressort de l'infrastructure critique concernée et ne font pas partie de la mission du NCSC. Le NCSC intervient subsidiairement aux services informatiques disponibles sur le marché, pour autant qu'il s'agisse d'exploitants privés. L'élément déterminant n'est pas la forme juridique de l'infrastructure, mais qui en est responsable. Le caractère subsidiaire du soutien apporté aux exploitants privés a pour but d'éviter que l'aide du NCSC ne débouche sur une distorsion de la concurrence sur le marché des services informatiques.

Si l'infrastructure critique concernée est assujettie à l'obligation de signaler en vertu des art. 74*b* et 74*c*, elle a droit au soutien technique du NCSC (cf. art. 74*a*, al. 4). Dans ce cas aussi, la réserve selon laquelle le NCSC ne doit pas concurrencer les prestataires de services informatiques s'applique lorsque le bénéficiaire est une organisation privée. Le NCSC soutient donc les assujettis à l'obligation de signaler, même si ce sont des organisations privées, dans la gestion des cyberincidents lorsqu'il n'est pas possible d'obtenir en temps utile une prestation équivalente sur le marché.

Al. 4

En cas de cyberincident, notamment sous la forme d'une cyberattaque, le NCSC a la possibilité d'accéder aux systèmes de l'infrastructure critique concernée afin de gérer l'incident ou de limiter les dommages, sous réserve que l'exploitant de l'infrastructure critique ait donné son consentement. Il appartient à l'exploitant de s'assurer qu'aucune obligation de garder le secret ne s'oppose à ce consentement. Dans la pratique, il est exceptionnel que le NCSC accède directement aux moyens informatiques d'une infrastructure critique. En règle générale, il collabore avec les spécialistes informatiques de l'entité concernée en leur fournissant des recommandations sur les indicateurs à rechercher au sein des systèmes.

Section 2: Obligation de signaler les cyberattaques

Art. 74a Principes

L'art. 74*a* règle la portée de l'obligation de signaler, le déroulement du signalement, l'assujettissement à l'obligation de signaler et le soutien du NCSC dans la gestion d'un cyberincident. Le NCSC assume la fonction de guichet de signalement pour les cyberattaques visées par l'obligation de signaler, comme il le fait déjà pour les signalements volontaires de cyberincidents et de cybermenaces.

Al. 1

L'al. 1 fixe l'obligation de signaler, le cercle des assujettis et le guichet de signalement. Les assujettis à l'obligation de signaler sont tenus de signaler au NCSC les cyberattaques visant leurs moyens informatiques. Le cercle des assujettis à l'obligation de signaler est détaillé à l'art. 74*b* et les exceptions seront précisées dans les dispositions d'exécution, conformément à l'art. 74*c*.

En vertu de l'art. 74*d*, les cyberattaques ne doivent être signalées que si elles visent les moyens informatiques des assujettis eux-mêmes. Ainsi, les fournisseurs de services Internet ne sont pas tenus de signaler les incidents concernant leurs clients.

L'obligation de signaler est aussi remplie lorsque les assujettis mandatent un tiers, par exemple l'exploitant de leurs moyens informatiques, pour effectuer les signalements. Si le même fournisseur de services informatiques travaille pour plusieurs assujettis, il peut se faire mandater par plusieurs d'entre eux pour signaler au NCSC les éventuelles cyberattaques visant leurs moyens informatiques respectifs. Compte tenu du court délai imparti pour effectuer le signalement (24 heures, conformément à l'art. 74*e*, al. 1), les assujettis à l'obligation de signaler devront cependant mandater les éventuels tiers de manière anticipée. En effet, après la découverte d'une cyberattaque, il reste peu de temps pour faire le signalement et la gestion de l'incident mobilise déjà beaucoup de ressources.

Lorsqu'un assujetti à l'obligation de signaler mandate un tiers pour effectuer le signalement, il ne lui transfère pas l'obligation de signaler en tant que telle. Un tel mandat ne change rien à l'assujettissement à l'obligation de signaler. Si le mandataire omet de signaler une cyberattaque au NCSC, l'assujetti doit répondre d'une éventuelle violation de son obligation de signaler.

Al. 2

Les domaines touchés par l'obligation de signaler énumérés à l'art. 74*b*, al. 1, étant nombreux, il est probable que certaines organisations auront quand même de la difficulté à déterminer si elles sont assujetties à l'obligation de signaler ou non, et ce malgré les précisions qui seront apportées au niveau de l'ordonnance. Afin que ces incertitudes ne leur portent pas préjudice et n'entachent pas l'efficacité de la nouvelle obligation de signaler, le NCSC renseignera, dans les cas limites, les autorités et les organisations intéressées – si possible au moyen d'un formulaire électronique – au sujet de leur assujettissement à ladite obligation. Si l'appréciation du NCSC est mise en doute ou contestée par l'entité concernée, le NCSC rendra une décision formelle, avec indication des voies de droit.

Al. 3

L'assujettissement à l'obligation de signaler ne doit pas seulement impliquer le moins de charge de travail possible pour les autorités et les organisations intéressées, mais doit aussi leur apporter des avantages concrets. Ainsi, les assujettis à l'obligation de signaler qui détectent une cyberattaque contre leurs moyens informatiques et qui la signalent dûment et dans les délais ont droit au soutien du NCSC dans la gestion de l'incident, comme prévu à l'art. 74, al. 3. En cas de capacités restreintes, le NCSC devra donc soutenir en priorité les assujettis à l'obligation de signaler.

Le droit au soutien du NCSC garantit aux assujettis que les avantages découlant de l'obligation de signaler l'emporteront sur l'éventuel surcroît de travail que celle-ci occasionnera, et qu'ils n'en retireront pas seulement une contrepartie, mais peut-être même une plus-value.

Al. 4

L'obligation de signaler a pour but de permettre au NCSC de détecter à un stade précoce les modes opératoires utilisés lors des attaques contre les infrastructures critiques et, ainsi, d'avertir les victimes potentielles et de leur recommander les mesures préventives et réactives qui s'imposent. La recommandation des mesures préventives et réactives fait partie des tâches légales du NCSC.

Le NCSC n'a aucune fonction de surveillance à l'égard des assujettis à l'obligation de signaler. L'obligation de signaler les cyberattaques n'est donc pas un instrument de contrôle[37]. Cette obligation est un outil précieux grâce auquel le NCSC est informé des attaques de manière précoce, ce qui lui permet d'améliorer la cybersécurité des infrastructures critiques au moyen de mesures préventives et réactives ciblées.

Le but de l'obligation de signaler implique que celle-ci doit être limitée aux cyberattaques. Les signalements de cyberincidents dus à de fausses manipulations ou à des dysfonctionnements ne sont d'aucun intérêt pour les alertes en matière de cybersécurité. Les signalements de cybermenaces, notamment des vulnérabilités, ne sont pas non plus visés par l'obligation de signaler (ch. 4.1).

Bien que, dans la plupart des cas, une cyberattaque débouche aussi sur une violation de la sécurité des données, l'obligation de signaler les cyberattaques poursuit un autre objectif que l'obligation d'annonce prévue dans le droit de la protection des données (cf. art. 24 nLPD). D'autres obligations de signaler, comme celles qui sont prévues dans les secteurs de la sécurité aérienne ou de la sécurité nucléaire, visent à couvrir autant que possible l'ensemble des erreurs, y compris les plus petites, dans l'optique d'une culture de sécurité. L'obligation de signaler les cyberattaques, quant à elle, ne vise pas des erreurs, raison pour laquelle la « culture juste »[38], ou « culture de l'équité », ne s'applique pas en matière de sanctions.

Art. 74b Autorités et organisations assujetties à l'obligation de signaler

D'un point de vue conceptuel, le champ d'application de l'obligation de signaler englobe les domaines qui, sous l'angle de la cybersécurité, représentent des cibles particulièrement intéressantes pour les cyberpirates. La liste exhaustive dressée à l'art. 74*b* se fonde sur les sous-secteurs critiques définis dans la stratégie nationale de protection des infrastructures critiques 2018-2022 (stratégie nationale PIC)[39] et, plus

37 La situation est différente, dans le secteur financier, s'agissant de l'obligation de signaler à la FINMA, puisque celle-ci est simultanément l'autorité de surveillance des assujettis à l'obligation de signaler.

38 Selon la définition donnée sur le site JustCulture.ch, la *just culture* est «une culture dans laquelle les employés des opérations ou d'autres services ne sont pas tenus responsables des actes, des omissions ou des décisions considérés comme appropriés au vu de leur expérience et de leur formation, mais dans laquelle les actes relevant d'une négligence grave, les actes intentionnels et les actions destructrices ne sont pas tolérés».

39 FF **2018** 491

particulièrement, sur les constats dressés par l'Office fédéral de la protection de la population (OFPP), responsable de la mise en œuvre de la stratégie nationale PIC.

La définition des infrastructures critiques est très ouverte, de sorte que presque tous les assujettis à l'obligation de signaler peuvent également être qualifiés d'infrastructures critiques au sens de l'art. 5, let. c, LSI[40].

Le champ d'application de l'obligation de signaler est délimité, dans la mesure du possible, avec des renvois aux bases légales existantes. Dans les domaines où un tel renvoi n'est pas possible – car il n'existe pas de bases légales appropriées pour une telle délimitation – le domaine concerné est décrit aussi précisément que possible. Cette approche a pour but de définir clairement, au niveau de la loi, le cercle des assujettis à l'obligation de signaler.

Compte tenu de la définition large du cercle des assujettis, il est peu probable qu'il faille compléter cette énumération dans les années à venir. Le Conseil fédéral pourra concrétiser et préciser davantage le cercle des assujettis dans les dispositions d'exécution, et ce individuellement pour chacun des domaines. Si, malgré tout, la situation demeure incertaine pour un intéressé, le NCSC a la possibilité de clarifier les cas limites en consultant l'OFPP et les autorités de surveillance et de régulation du secteur concerné, et de rendre une décision sur l'assujettissement à l'obligation de signaler (art. 74*a*, al. 2).

Enfin, le Conseil fédéral fixera des exceptions à l'obligation de signaler au sein de certains domaines au moyen de valeurs seuils. Il est donc tenu de veiller à la proportionnalité de l'obligation de signaler en exemptant les organisations qui ne sont pas essentielles pour le fonctionnement de l'économie ou pour le bien-être de la population (art. 74*c*).

Al. 1

Let. a: hautes écoles

Les hautes écoles sont d'une grande importance pour la formation et l'économie en Suisse. Leurs activités de recherche, en particulier, constituent un moteur de l'innovation. De ce fait, elles sont également une cible privilégiée pour les cyberattaques. Les universités cantonales, les écoles polytechniques fédérales, les hautes écoles spécialisées et les hautes écoles pédagogiques sont soumises à l'obligation de signaler.

Let. b: autorités

Les cyberattaques contre les autorités de tous les niveaux fédéraux doivent être signalées, car il est important de savoir à quelle fréquence et par qui elles sont attaquées. Les dispositifs de défense peuvent ainsi être adaptés aux menaces en cause. Les autorités visées incluent le Parlement fédéral et les parlements cantonaux.

40 À l'art. 5, let. c, LSI, les infrastructures critiques sont définies comme suit: « l'approvisionnement en eau potable et en énergie, les infrastructures d'information, de communication et de transports ainsi que d'autres installations, processus et systèmes essentiels au fonctionnement de l'économie et au bien-être de la population ».

Le Groupement Défense du Département fédéral de la défense, de la protection de la population et des sports (DDPS) est exempté de l'obligation de signaler lorsque l'armée accomplit un service d'appui ou un service actif au sens respectivement des art. 67 et 76 de la loi du 3 février 1995 sur l'armée[41]. L'obligation de signaler pourrait dans ce cas mettre en péril des secrets militaires ou entraver la collaboration avec les organisations partenaires.

Let. c: organisations actives dans les domaines de la sécurité et du sauvetage, de l'approvisionnement en eau potable, du traitement des eaux usées et de l'élimination des déchets

Les organisations qui assument des tâches de droit public dans certains domaines sont assujetties à l'obligation de signaler. La let. c énumère les activités concrètement visées ici. Dans le domaine de la sécurité et du sauvetage, l'accent est mis sur les organisations d'intervention d'urgence (police, services du feu, services sanitaires et services de sauvetage). Les organisations chargées de l'approvisionnement en eau potable, du traitement des eaux usées et de l'élimination des déchets sont également assujetties. L'obligation de signaler ne s'applique toutefois qu'aux tâches relevant de la puissance publique de ces autorités et de ces organisations.

Let. d: entreprises œuvrant dans les domaines de l'approvisionnement énergétique ainsi que du commerce, de la mesure et de la gestion de l'énergie

L'approvisionnement en énergie est essentiel pour l'économie et la société. Des attaques menées contre l'approvisionnement en électricité ou contre des pipelines dans d'autres États ont montré que ces infrastructures font l'objet d'attaques ciblées, que ce soit pour des motifs politiques ou pour extorquer des sommes aussi élevées que possible. Les entreprises dont les activités sont importantes pour l'approvisionnement en énergie sont donc assujetties à l'obligation de signaler. Selon l'art. 6, al. 1, de la loi du 30 septembre 2016 sur l'énergie[42], l'approvisionnement énergétique comprend «la production, la transformation, le stockage, la fourniture, le transport, le transfert et la distribution d'énergie et d'agents énergétiques jusqu'à leur livraison au consommateur final, y compris l'importation, l'exportation et le transit». La let. d vise également les entreprises qui sont actives dans le commerce, la mesure ou la gestion de l'énergie.

Les détenteurs d'une autorisation au sens de la loi du 21 mars 2003 sur l'énergie nucléaire (LENu)[43] sont exemptés de l'obligation de signaler les cyberattaques si une cyberattaque est lancée contre une installation nucléaire. Ils sont déjà soumis à des obligations de déclarer de grande portée à l'égard de l'IFSN pour les événements susceptibles de mettre en cause la sécurité nucléaire et la sûreté, y compris en ce qui concerne les cyberattaques contre les installations nucléaires (art. 22, al. 2, let. f, LENu en relation avec les art. 38, al. 3, et 39, al. 2, de l'ordonnance du 10 décembre 2004 sur l'énergie nucléaire[44]).

41 RS **510.10**
42 RS **730.0**
43 RS **732.1**
44 RS **732.11**

En sa qualité d'autorité fédérale de surveillance des installations nucléaires suisse, l'IFSN s'est dotée d'un guichet de signalement sectoriel qui dispose d'une organisation prête à intervenir à tout instant avec un personnel technique qualifié, y compris dans le domaine de la cybersécurité. Les processus de signalement mis en place sont bien établis et ont été testés afin qu'ils fonctionnent de manière fiable en cas d'événement dans une installation nucléaire.

Il convient donc de renoncer à introduire une obligation de signaler supplémentaire pour les détenteurs d'une autorisation au sens de la LENu, ce afin d'exclure tout risque d'entraver les processus sensibles et bien établis, propres à la sécurité nucléaire, en cas d'événement. En revanche, un nouvel art. 102, al. 2, LENu oblige l'IFSN à transmettre au NCSC les éventuels signalements qu'elle reçoit concernant les cyberattaques contre les installations nucléaires qui remplissent les conditions posées à l'art. 74*d*.

Let. e: banques, assurances et infrastructures des marchés financiers

Les entreprises du secteur financier sont fortement touchées par les cyberattaques, car elles représentent une cible intéressante pour les criminels en raison des moyens financiers considérables qu'elles gèrent. Pour la fiabilité de la place financière suisse, il est important que ces cyberattaques soient signalées. L'obligation de signaler les cyberattaques à la FINMA, qui existe déjà, reste en vigueur parallèlement à la nouvelle obligation de signaler au NCSC. La FINMA et le NCSC assureront la coordination afin que la charge de travail pour les assujettis à ces obligations reste la plus faible possible.

Let. f: établissements de santé

Un hôpital est un établissement de santé qui propose en milieu hospitalier au moyen de prestations d'assistance médicale et de soins soit un traitement de maladies, soit des mesures médicales de réadaptation, soit des mesures médicales à des fins esthétiques (art. 4, al. 1, let. l, de l'ordonnance du 1er juillet 2020 sur les dispositifs médicaux[45]). Toutefois, seuls les hôpitaux figurant sur la liste hospitalière de leur canton (art. 39, al. 1, let. e, de la loi fédérale du 18 mars 1994 sur l'assurance-maladie [LAMal][46]) sont assujettis à l'obligation de signaler.

Les hôpitaux de soins aigus, de réadaptation et de psychiatrie qui figurent sur les listes hospitalières cantonales assurent la couverture des besoins en soins médicaux de base sur le territoire du canton concerné. Ces listes peuvent aussi contenir des maisons de naissance et des établissements médico-sociaux (art. 39, al. 3, LAMal). L'obligation de signaler les cyberattaques doit s'appliquer à tous les établissements de santé de la liste, car il s'agit d'éviter que ce genre d'attaques ne compromettent la fourniture des soins de base. Si des cyberattaques visant des établissements de santé ou l'Office fédéral de la santé publique entraînent la mise en péril de données contenues dans des dossiers électroniques de patients, l'obligation de signaler l'événement incombe à l'organisation visée par la cyberattaque.

45 RS **812.213**
46 RS **832.10**

Let. g: laboratoires médicaux

Les laboratoires qui effectuent des analyses microbiologiques pour détecter des maladies transmissibles sont importants pour les soins de santé. Pour leurs analyses et leur collaboration avec les médecins de premier recours, ils dépendent dans une large mesure du bon fonctionnement de l'infrastructure informatique. Les cyberattaques visant ces laboratoires doivent donc être visées par l'obligation de signaler.

Let. h: fabrication, mise sur le marché et importation de médicaments

La fabrication, la mise sur le marché et l'importation de médicaments revêtent une grande importance pour les soins médicaux prodigués à la population. Les entreprises actives dans ces domaines et titulaires d'une autorisation au sens de la loi du 15 décembre 2000 sur les produits thérapeutiques[47] sont donc assujetties à l'obligation de signaler.

Let. i: assurances sociales

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 sont elles aussi assujetties à l'obligation de signaler. Le projet n'utilise pas l'expression « assurances sociales », car cette notion n'est pas définie dans la législation. La portée de l'obligation de signaler est donc définie sur la base des prestations octroyées pour les risques prévus par la loi fédérale du 6 octobre 2000 sur la partie générale du droit des assurances sociales (LPGA)[48] afin de couvrir, dans la mesure du possible, toutes les branches des assurances sociales. L'obligation de signaler n'est cependant pas limitée aux assurances sociales qui sont soumises à la LPGA. Il a été choisi de ne pas dresser une liste des différentes lois (par ex. loi fédérale du 19 juin 1959 sur l'assurance-invalidité[49] ou loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants[50]) pour englober non seulement les prestations légales, mais aussi les prestations surobligatoires telles que la prévoyance professionnelle ou l'assurance complémentaire à l'assurance-maladie obligatoire.

Dans le domaine de la prévoyance professionnelle (deuxième pilier), l'obligation de signaler s'étend à toutes les institutions de prévoyance enregistrées ou non enregistrées (y c. institutions supplétives), aux institutions de libre passage et au Fonds de garantie LPP

Les offres de prévoyance individuelle (pilier 3a et 3b) sont généralement proposées par les banques et les assurances, qui sont elles-mêmes assujetties à l'obligation de signaler.

Dans le cas des assurances sociales également, le Conseil fédéral pourra restreindre au niveau de l'ordonnance le cercle des assujettis à l'obligation de signaler et, par exemple, limiter par des critères appropriés le cercle des institutions de prévoyance et de libre passage assujetties (art. 74*c* et explications sous ch. 4.3.3).

47 RS **812.21**
48 RS **830.1**
49 RS **831.20**
50 RS **831.10**

Let. j: Société suisse de radiodiffusion et télévision (SSR)

La Société suisse de radiodiffusion et télévision (SSR) a pour mandat de fournir à l'ensemble de la population des programmes de radio et de télévision complets et de même valeur dans les trois langues officielles. Elle a également pour mission de contribuer à la libre formation de l'opinion en présentant une information complète, diversifiée et fidèle, en particulier sur les réalités politiques, économiques et sociales (art. 24, al. 1, let. a, et art. 4, let. a, de la loi du 24 mars 2006 sur la radio et la télévision[51]). Son mandat va donc nettement plus loin que les obligations d'information des autres médias titulaires d'une concession, ce qui fait d'elle une cible intéressante pour des cyberattaques. Cela justifie l'assujettissement de la SSR à l'obligation de signaler.

Let. k: agences de presse d'importance nationale

Une agence de presse est qualifiée d'importance nationale (au sens de l'art. 44*a* de l'ordonnance du 9 mars 2007 sur la radio et la télévision[52]) lorsque les informations diffusées portent sur les quatre régions linguistiques et se font régulièrement dans trois langues nationales (art. 18, let. a, de la loi du 5 octobre 2007 sur les langues[53] en relation en relation avec l'art. 13 de l'ordonnance du 4 juin 2010 sur les langues[54]). La dernière agence de presse encore active en Suisse est Keystone-ATS (ordonnance COVID-19 du 20 mai 2020 médias électroniques[55]).

Let. l: prestataires de services postaux

Les entreprises qui offrent des services postaux à des clients en leur propre nom sont également assujetties à l'obligation de signaler si elles sont enregistrées auprès de la Commission de la poste conformément à l'art. 4, al. 1, de la loi du 17 décembre 2010 sur la poste (LPO)[56]. Le Conseil fédéral pourra exempter les petites entreprises de l'obligation de signaler au niveau de l'ordonnance. On pourrait, par exemple, envisager une restriction analogue à celle prévue à l'art. 4, al. 2, LPO pour les entreprises qui réalisent un faible chiffre d'affaires.

Let. m: transports publics (transport de voyageurs et transport ferroviaire de marchandises)

Le renvoi aux deux lois fédérales pertinentes (loi fédérale du 20 décembre 1957 sur les chemins de fer[57] et loi du 20 mars 2009 sur le transport de voyageurs [LTV][58]) permet de couvrir les secteurs les plus importants que sont le transport public de voyageurs, le transport ferroviaire de marchandises et l'infrastructure ferroviaire. Cette disposition ne vise donc pas les petites entreprises d'autocar ou d'installations à câbles qui sont au bénéfice d'une autorisation cantonale (art. 7 LTV). Le transport de voya-

51 RS **784.40**
52 RS **784.401**
53 RS **441.1**
54 RS **441.11**
55 RS **784.402**
56 RS **783.0**
57 RS **742.101**
58 RS **745.1**

geurs transfrontalier n'est pas non plus concerné. La mention spécifique des entreprises de transport ferroviaire est nécessaire dans la mesure où le transport ferroviaire des marchandises n'est pas soumis à un régime de concession.

Let. n: entreprises de l'aviation civile

Les entreprises de l'aviation civile qui disposent d'une autorisation délivrée par l'Office fédéral de l'aviation civile (par ex. une autorisation d'exploitation au sens de l'art. 27 de la loi fédérale du 21 décembre 1948 sur l'aviation [LA][59]) et les aéroports nationaux figurant dans le Plan sectoriel de l'infrastructure aéronautique (PSIA) doivent eux aussi être assujettis à l'obligation de signaler les cyberattaques.

La LA mentionne seulement les aéroports nationaux de Zurich et de Genève (art. 37*u*, al. 2, LA), mais pas celui de Bâle. Il a donc paru nécessaire de renvoyer au PSIA afin d'englober tous les aéroports nationaux. Le Conseil fédéral adopte une fiche d'objet PSIA pour chaque aéroport national (Zurich, Genève, Bâle). Le Département fédéral de l'environnement, des transports, de l'énergie et de la communication est l'autorité chargée de l'approbation des plans pour les aéroports (art. 37 ss LA).

Let. o: port de Bâle et navigation sur le Rhin

Les Ports rhénans suisses constituent le seul débouché maritime de la Suisse. Ils sont d'une grande importance pour l'approvisionnement du pays en marchandises de toutes sortes. L'obligation de signaler les cyberattaques s'applique donc à la navigation sur le Rhin pour le transport de marchandises conformément à la loi fédérale du 23 septembre 1953 sur la navigation maritime sous pavillon suisse[60] et aux processus importants pour l'exploitation et le fonctionnement du port de Bâle.

Let. p: biens d'usage quotidien indispensables

Une multitude d'opérateurs sont impliqués dans l'approvisionnement de la population en biens d'usage quotidien indispensables, notamment en denrées alimentaires. Outre les producteurs et les importateurs, les transformateurs, les centres de distribution et les détaillants jouent également un rôle important. Tous ces opérateurs n'ont pas la même importance pour la sécurité de l'approvisionnement de la Suisse. C'est la raison pour laquelle il est proposé de restreindre la portée de la loi aux seules entreprises dont la défaillance partielle ou complète entraînerait de graves difficultés d'approvisionnement.

L'obligation de signaler les cyberattaques ne s'appliquera donc qu'aux opérateurs qui jouent un rôle important pour l'approvisionnement économique de la Suisse. Le Conseil fédéral limitera donc l'obligation de signaler dans le domaine de l'approvisionnement en biens d'usage quotidien indispensables au niveau de l'ordonnance en se fondant sur les critères définis à l'art. 74*c*.

Let. q: fournisseurs de services de télécommunication

Par transmission au moyen de techniques de télécommunication, on entend l'émission ou la réception d'informations, sur des lignes ou par ondes hertziennes, au moyen de

59 RS **748.0**
60 RS **747.30**

signaux électriques, magnétiques ou optiques ou d'autres signaux électromagnétiques (art. 3, let. c, de la loi du 30 avril 1997 sur les télécommunications [LTC][61]). Est également considérée comme une transmission au moyen de techniques de télécommunication l'offre de capacité de transmission.

Quiconque transmet des informations pour le compte de tiers est considéré comme un fournisseur de services de télécommunication. Seuls les fournisseurs de services de télécommunication enregistrés au sens de l'art. 4 LTC sont assujettis à l'obligation de signaler,

Let. r: registres et registraires de domaines Internet

Les noms de domaine Internet permettent d'attribuer une adresse unique à chaque site Internet. Ces noms, par exemple ofcom.ch, sont surtout utilisés pour accéder à des sites Internet et pour envoyer des courriers électroniques.

Au niveau mondial, les noms de domaine Internet sont gérés par l'Internet Corporation for Assigned Names and Numbers (ICANN). La Confédération gère les noms de domaines du premier niveau qui ont un lien avec la Suisse (art. 28*b* ss LTC).

L'Office fédéral de la communication exerce la fonction de registre (*registry*), étant entendu qu'il a délégué cette tâche à l'entreprise SWITCH. Sous certaines conditions, il peut agir en qualité de registraire (*registrar*) lorsqu'il n'y a pas d'offre satisfaisante sur le marché. Le registre est responsable de la gestion technique et opérationnelle centralisée pour les domaines «.ch» et «.swiss», tandis que la fonction de registraire peut être exercée par plusieurs entreprises qui se chargent de commercialiser les noms de domaine sur le marché libre (ordonnance du 5 novembre 2014 sur les domaines Internet [ODI][62]).

Les registraires qui ont conclu un contrat de registraire avec le registre peuvent requérir et gérer des noms de domaine pour leurs clients. Les registraires ont donc un rôle d'interface exclusive entre le registre et les requérants (art. 24, al. 1, et annexe, let. m, ODI).

Let. s: droits politiques

Les services et infrastructures servant à l'exercice des droits politiques comprennent les systèmes utilisés pour récolter et compter les signatures dans le cadre de requêtes populaires (initiatives populaires, référendums, pétitions, etc.), ainsi que pour préparer, exécuter et dépouiller les scrutins.

Cela comprend, par exemple, les systèmes de vote électronique (*e-voting*), de gestion des registres électoraux ou d'établissement et de transmission des résultats des scrutins. À l'avenir, cela pourrait aussi inclure des systèmes électroniques de récolte de signatures (*e-collecting*). Les entreprises chargées d'imprimer le matériel de vote, par exemple, font ELLES aussi partie des services et infrastructures visés.

61 RS **784.10**
62 RS **784.104.2**

Let. t: services numériques

L'obligation de signaler s'applique aux fournisseurs et exploitants d'informatique en nuage (par ex. *software as a service,* ou SaaS), de moteurs de recherche, de services numériques de sécurité ou de confiance et de centres de calcul, pour autant qu'ils aient un siège en Suisse.

Par analogie avec le droit européen[63], la notion de «service de confiance» inclut les services de signature électronique, de cachet ou d'horodatage électroniques, d'envoi recommandé électronique, de certificats d'authentification ainsi que de conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services. L'identité électronique (e-ID) est, par exemple, également considérée comme un service de confiance.

Par «services de sécurité», on entend notamment les solutions de chiffrement des informations ainsi que les moyens informatiques qui servent à se protéger contre les cyberattaques (filtres antipourriels, programmes antivirus, pare-feu).

Let. u: fabricants de matériel informatique et de logiciels

Les cyberattaques visant les infrastructures critiques à travers leur chaîne d'approvisionnement font désormais partie des menaces importantes. Cela concerne tout particulièrement les fournisseurs de matériel informatique et de logiciels. Les pirates manipulent les moyens informatiques avant leur livraison aux clients finaux afin de pouvoir accéder ultérieurement aux systèmes. Les cyberattaques contre les fabricants de matériel informatique et de logiciels qui fournissent les infrastructures critiques revêtent donc une grande importance pour la cybersécurité.

Les cyberattaques contre ces fabricants sont particulièrement importantes lorsque ceux-ci disposent d'un accès aux systèmes pour la télémaintenance. Un accès de télémaintenance permet à un fabricant, lorsqu'il dispose des droits nécessaires, d'accéder depuis l'extérieur (généralement via Internet) aux composants informatiques et de technologie opérationnelle du réseau local à des fins de maintenance ou de dépannage. Les pirates peuvent tenter de s'introduire directement dans les systèmes des infrastructures critiques par ce genre d'accès légitime.

Outre le critère de l'accès de télémaintenance, les fabricants de matériel informatique et de logiciels sont aussi soumis à l'obligation de signaler lorsque leurs produits sont utilisés dans des domaines particulièrement sensibles. Cela concerne le matériel informatique et les logiciels utilisés pour commander et surveiller des appareils physiques, des processus et des événements (techniques opérationnelles, ou *operational technology*). Sont compris notamment les systèmes de contrôle industriels (*industrial control systems*) ainsi que les solutions d'automatisation, qui remplissent toutes sortes de fonctions de contrôle et de réglage. On peut encore penser aux appareils de laboratoire tels que les microscopes ou les instruments d'analyse automatiques, aux systèmes logistiques comme les lecteurs de codes-barres avec mini-ordinateur, ou encore aux systèmes de gestion d'immeuble (ch. 1).

63 Le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JO L 257 du 28.8.2014, p. 73, définit ce qu'est un «service de confiance» à l'art. 3, ch. 16.

Le matériel informatique et les logiciels utilisés pour garantir la sécurité publique sont également visés (ch. 2). On pense ici, en particulier, à la communication des organisations d'intervention d'urgence ou aux systèmes d'enquête policière.

Al. 2

Les grandes entreprises, les conglomérats et les groupes qui déploient une partie de leurs activités dans l'un des secteurs énumérés à l'al. 1 ne sont pas assujettis à l'obligation de signaler pour toutes leurs activités, mais uniquement pour celles qui relèvent des secteurs mentionnés à l'al. 1. Par exemple, si une entreprise de denrées alimentaires exploite aussi un parc de loisirs, ou qu'un établissement financier gère parallèlement un musée, l'entreprise doit signaler une cyberattaque dont elle est victime uniquement si celle-ci visait les moyens informatiques utilisés respectivement dans le secteur des denrées alimentaires ou dans celui des services financiers.

Al. 3

Les entreprises et les organisations assujetties qui déploient leurs activités à l'international peuvent légitimement se demander si elles doivent aussi signaler les cyberattaques lorsque les moyens informatiques visés se situent à l'étranger. La réponse est oui dès lors que l'assujetti a un siège en Suisse, qu'il exerce une activité dans l'un des domaines énumérés à l'al. 1 et que les moyens informatiques visés par la cyberattaque servent à exercer cette activité en Suisse.

Art. 74c Exceptions à l'obligation de signaler

Le cercle des assujettis à l'obligation de signaler défini à l'art. 74*b* est large. Il peut aussi englober des organisations et des autorités qui, prises individuellement, ne sont pas essentielles au bon fonctionnement de l'économie ou au bien-être de la population (en raison de leur taille ou de leur degré de contribution à l'approvisionnement), bien qu'elles soient actives dans un sous-secteur critique mentionné à l'art. 74*b*, al. 1.

L'art. 74*c* précise donc que le Conseil fédéral devra restreindre le cercle des assujettis au niveau de l'ordonnance. Une exemption de l'obligation de signaler est ainsi prévue lorsqu'une défaillance de l'organisation ou de l'autorité n'aurait qu'un faible impact sur le fonctionnement de l'économie ou sur le bien-être de la population. L'impact se mesure ici à l'aune du nombre de personnes.

Art. 74d Cyberattaques à signaler

La portée de l'obligation de signaler, c'est-à-dire les types de cyberattaques qui doivent être signalés, doit être fixée dans la loi. Les let. a à d énumèrent les critères permettant de déterminer les cyberattaques qui sont particulièrement pertinentes pour l'alerte précoce et l'appréciation de la menace, et qui doivent donc être signalées. Les critères ont été définis de façon à pouvoir être appliqués le plus directement possible par les entreprises. Ils pourront, au besoin, être précisés dans l'ordonnance.

Let. a

La mise en péril du fonctionnement de l'infrastructure critique est le seul critère qui ne soit pas axé sur la pertinence pour la cybersécurité, mais sur les effets. Ce critère a été choisi parce que le potentiel de dommage est déterminant pour faire valoir le droit

au soutien du NCSC lors de la gestion de l'incident (cf. art. 74*a*, al. 4, en relation avec l'art. 74, al. 3).

Let. b

La manipulation des informations est un critère qui rend le signalement d'une cyberattaque obligatoire. Par manipulation, on entend par exemple le chiffrement d'informations de l'organisation concernée.

Let. c

Lorsqu'une cyberattaque n'a pas été détectée pendant une période prolongée, on ne peut pas exclure une activité d'espionnage (par ex. industriel) ou le fait que l'attaque ait été menée en vue de préparer d'autres cyberattaques. Les informations sur les attaques conçues intentionnellement pour être détectées le plus tard possible sont particulièrement importantes dans l'optique de l'alerte des autres exploitants d'infrastructures critiques.

Let. d

Une cyberattaque doit toujours être signalée lorsqu'elle s'accompagne d'actes pénalement répréhensibles. De nombreux cybercriminels tentent de faire chanter les exploitants d'infrastructures critiques, les clients ou certains des collaborateurs de ces derniers en menaçant de lancer des attaques ou en les exécutant (par ex. en chiffrant les données à l'aide d'un rançongiciel [*ransomware*], en menaçant de compromettre la disponibilité au moyen d'attaques de déni de service distribué [DDoS] ou en menaçant de publier des informations compromettantes sur des personnes).

Les cyberattaques qui s'accompagnent d'actes pénalement répréhensibles doivent être signalées lorsque le chantage, la menace ou la contrainte a un rapport avec l'entreprise assujettie et que ces actes sont susceptibles d'avoir des effets négatifs sur la marche des affaires de l'entreprise. Il est important de signaler ce type d'attaques afin qu'il soit possible d'évaluer l'ampleur de la menace que les cybercriminels font peser sur les infrastructures critiques.

Art. 74e *Délai et contenu du signalement*

Al. 1

Il est essentiel pour l'alerte précoce et la prévention que les attaques soient signalées immédiatement après leur découverte. Un délai de signalement de 24 heures tient compte de cette nécessité. Seules les informations recueillies durant ce laps de temps doivent être communiquées dans les 24 heures; le signalement pourra être complété par la suite[64].

64 Cf. communication FINMA sur la surveillance n° 05/2020, consultable en ligne sous www.finma > Documents > Communications FINMA sur la surveillance.

Al. 2

Le contenu du signalement, soit les informations essentielles à fournir pour satisfaire à l'obligation de signaler, est décrit à l'al. 2. La portée et la teneur concrètes des informations devront être précisées dans les dispositions d'exécution. Le NCSC décrira en outre de manière détaillée, dans le formulaire de signalement, à quoi correspondent les différentes informations exigées. Par «type et exécution de la cyberattaque», on entend par exemple les *indicators of compromise* (IOC). Il s'agit notamment des adresses IP ou des *DNS records* d'infrastructures de piratage connues (par ex. ceux des réseaux de machines zombies [*botnet*] ou de serveurs de commande et de contrôle [*C&C server*]), des URL de pages douteuses, des valeurs de hachage (*hash value*) de maliciels, des signatures virales, des anomalies du trafic réseau ou encore des comportements anormaux de logiciels. L'expression «mesures prises» est la même que celle utilisée à l'art. 24, al. 2, nLPD.

Pour satisfaire à l'obligation de signaler, il n'est pas nécessaire de communiquer des informations concernant des secrets professionnels ou d'affaires des assujettis, ou qui violeraient de tels secrets, ni de fournir des informations susceptibles d'auto-incriminer l'auteur du signalement (al. 4).

Al. 3

Afin de limiter le plus possible la charge de travail des auteurs de signalements, seules les informations impérativement nécessaires doivent être fournies au moment de la détection de la cyberattaque. Lors d'une cyberattaque, on ignore très souvent pendant un certain temps à quel point l'attaque est grave et ce qui s'est passé précisément. Si ces informations sont incomplètes au moment du signalement, les entités concernées doivent par conséquent avoir la possibilité de ne transmettre les informations exigées conformément au ch. 2 que lorsqu'elles disposent de plus de détails sur la cyberattaque. Cette approche en deux temps est également valable pour l'obligation de signaler les cyberattaques à la FINMA. Il a été volontairement renoncé à fixer un deuxième délai de signalement afin que les intéressés puissent se concentrer sur la gestion de l'incident. En lieu et place de ce deuxième délai, il est prévu que le NCSC informe les assujettis à l'obligation de signaler lorsque toutes les informations requises ont été fournies et que ladite obligation peut donc être considérée comme remplie (al. 5).

Al. 4

En règle générale, les données qui doivent être transmises au NCSC dans le cadre de l'obligation de signaler ne contiennent pas d'informations susceptibles d'exposer l'assujetti ou l'auteur du signalement à des poursuites pénales. Pour s'assurer que le principe de l'interdiction de l'obligation de l'auto-incrimination reste garanti, cette circonstance est mentionnée au niveau de la loi. Une remarque à ce sujet est aussi prévue dans le formulaire de signalement.

Al. 5

Afin que les assujettis à l'obligation de signaler sachent clairement si les informations fournies sont complètes et suffisamment précises, le NCSC leur communiquera si les informations qu'il a reçues sont suffisamment exhaustives et claires et s'ils satisfont ainsi à l'obligation de signaler.

Art. 74f Communication du signalement

Al. 1

Afin que l'obligation de signaler puisse être remplie avec le moindre effort possible, il incombe au NCSC de mettre à disposition un système électronique sécurisé pour la communication des signalements, par exemple au moyen d'un formulaire dédié qui sera structuré de la même manière que le formulaire utilisé actuellement pour la déclaration volontaire des cyberincidents et des cybermenaces. Compte tenu des développements technologiques, le formulaire est décrit de manière générique comme «un système […] qui permet de […] communiquer le signalement».

Le NCSC offrira la possibilité de s'inscrire au préalable, de sorte que les assujettis à l'obligation de signaler n'auront pas à saisir les informations sur eux-mêmes lors de chaque signalement. Le principe dit *once only*, selon lequel les données des auteurs des signalements ne doivent être saisies qu'une seule fois, est ainsi mis en œuvre dans le cadre de l'obligation de signaler. Un signalement automatisé via une interface de programmation d'application (API) ne serait pas judicieux, car le NCSC recevrait un trop grand nombre d'informations. Il appartient aux assujettis à l'obligation de signaler de transmettre au NCSC uniquement les informations souhaitées en lien avec la cyberattaque.

En dehors de ce formulaire, il reste possible dans tous les cas de communiquer d'une autre manière (par courriel ou par téléphone) la cyberattaque au NCSC.

Al. 2 et 3

À la demande d'autres guichets de signalement et en collaboration avec eux, le NCSC aménagera le système de communication de manière à ce que l'auteur d'un signalement ait la possibilité de communiquer simultanément à d'autres autorités tout ou partie du signalement de la cyberattaque ou de ses effets (par ex. sur la sécurité des données ou sur le fonctionnement de l'infrastructure critique; al. 2), voire de leur communiquer des informations supplémentaires qui sont nécessaires à l'accomplissement d'autres obligations de signaler (al. 3). Cette fonction doit servir à réduire au minimum la charge de travail de l'auteur d'un signalement: en cas de cumul de plusieurs obligations de signaler, elle permettra à ce dernier d'informer les autorités concernées rapidement, en temps utile et avec le moins d'effort possible.

Il est important de noter que, en vertu de l'al. 2, seuls les assujettis à l'obligation de signaler peuvent communiquer tout ou partie du signalement à une autre autorité. Eux seuls déterminent quelles autorités – en dehors du NCSC – doivent recevoir la communication de la cyberattaque ou de ses effets.

Selon l'al. 3, les assujettis à l'obligation de signaler ont aussi la possibilité de saisir d'éventuelles données supplémentaires qui ne sont pas nécessaires pour le signalement au NCSC, et de les transmettre à un ou plusieurs autres guichets de signalement afin de remplir d'autres obligations de signaler. Les informations supplémentaires que les auteurs d'un signalement saisissent pour d'autres services et autorités dans le système de communication du NCSC sont uniquement transmises par ce dernier, sans être enregistrées. Le NCSC lui-même n'a pas la possibilité d'accéder à ces informations.

Le NCSC proposera aux guichets de signalement intéressés la possibilité de compléter son formulaire électronique en fonction de leurs besoins propres, afin de réduire la charge de travail pour les assujettis aux différentes obligations de signaler et d'exploiter ainsi des synergies. Cela ne remplacera pas les autres obligations de signaler et ne transformera pas le NCSC en guichet de signalement pour d'autres obligations de signaler. Cette fonction de communication à d'autres autorités tient néanmoins compte de la nécessité d'aménager un guichet de signalement permettant de remplir plusieurs obligations de signaler de même nature en une seule étape. Le NCSC n'exerce cependant aucun rôle actif dans la communication des informations aux autres guichets de signalement. La transmission est effectuée exclusivement par les assujettis à l'obligation de signaler.

Art. 74g Violation de l'obligation de signaler

Al. 1

En cas de violation de l'obligation de signaler, le NCSC doit, dans un premier temps, attirer l'attention des assujettis sur leur obligation de signaler. Ceux-ci ont ainsi encore l'occasion de s'acquitter de leurs obligations dans un délai approprié. S'il y a un malentendu à ce sujet, il est alors possible de le régler.

Pour prévenir des malentendus, le NCSC peut déjà demander des informations complémentaires aux assujettis s'il constate que les données fournies dans le signalement sont incomplètes ou imprécises. Il informe en outre les assujettis dès que les informations requises ont été fournies et que l'obligation de signaler peut être considérée comme remplie (art. 74*e*, al. 5).

Dans l'éventualité d'une violation de l'obligation de signaler, le NCSC se montrera donc pragmatique et il informera d'abord les assujettis de la violation de leurs obligations. Le NCSC est tenu de prendre ce premier contact. Cette obligation d'informer est une condition préalable au fait de rendre une décision en vertu de l'al. 2.

Al. 2

Dans un second temps, soit lorsque les assujettis à l'obligation de signaler n'agissent pas dans le délai imparti en dépit de la violation manifeste de leurs obligations, le NCSC rend une décision assortie d'une menace d'amende. Dans sa décision, le NCSC doit préciser les obligations qui ont été violées afin qu'il n'y ait aucun doute pour l'assujetti sur ce qu'il doit faire. Cela facilitera également le travail des autorités cantonales de poursuite pénale, qui, en cas d'insoumission à cette décision et sur dénonciation du NCSC, doivent établir les faits et rendre un arrêt ou une ordonnance pénale (art. 74*h*).

Art. 74h Insoumission à une décision du NCSC

Il a été opté pour un régime d'amendes qui reprend en grande partie le mécanisme prévu aux art. 60 ss nLPD en cas de violation d'une obligation ou d'insoumission à une décision du préposé. Dans le sens des explications données dans le message du 15 septembre 2017 concernant la loi fédérale sur la révision totale de la loi fédérale

sur la protection des données et sur la modification d'autres lois fédérales[65], il s'agit aussi dans le cas d'espèce de veiller à ce que soit punissable la personne responsable qui, au sein de l'infrastructure critique, aurait dû faire exécuter la décision du NCSC (cf. art. 29 CP). Le respect de l'obligation de signaler qui incombe en réalité à l'entreprise est ici imputé à cette personne physique.

Le renvoi à l'art. 6 de la loi fédérale du 22 mars 1974 sur le droit pénal administratif[66] permet d'attribuer la responsabilité pénale à la direction de l'entreprise, c'est-à-dire aux personnes occupant une fonction dirigeante et disposant de pouvoirs de décision et de direction. Cette imputation de la responsabilité pénale au sein des entreprises assujetties est appropriée et relève de l'organisation interne des assujettis à l'obligation de signaler.

Al. 1

Le montant maximal de l'amende a été fixé à 100 000 francs afin de tenir dûment compte de l'importance des infrastructures critiques pour le bon fonctionnement de la société, de l'économie et de l'État, et pour bien signaler la responsabilité de leurs exploitants dans le domaine de la cybersécurité. Un montant aussi élevé se justifie également par le fait que l'amende n'est prononcée qu'en dernier ressort, après toute une succession de mesures. Tant la disparité du niveau de cybersécurité d'un secteur à l'autre que les exigences supplémentaires liées au nouveau régime de signalement des cyberattaques ont conduit à ne pas reprendre le montant maximal de 250 000 francs prévu dans la loi révisée sur la protection des données. Il faut également admettre que les intérêts en présence et l'imputation de la responsabilité sont d'un tout autre ordre en cas de violation de la protection des données. La menace d'une amende de 100 000 francs devrait déjà amener les responsables des infrastructures critiques assujetties à agir en conformité avec leurs obligations.

La quotité de l'amende sera fixée en tenant compte de la situation personnelle de l'intéressé, conformément aux principes du droit pénal applicables.

Al. 2 et 3

Pour les amendes infligées à des entreprises, la réglementation de la loi révisée sur la protection des données (art. 64 nLPD) a été reprise par analogie. Le rapport entre le montant maximal de 20 000 francs pour les amendes infligées directement aux entreprises et le montant maximal de 100 000 francs prévu par la loi est le même que dans le droit de la protection des données (50 000 et 250 000 francs respectivement).

Jusqu'à un montant de 20 000 francs, l'amende peut donc être directement infligée à l'entreprise assujettie à la place de la personne physique responsable, afin d'éviter des actes d'instruction coûteux. Étant donné qu'une amende ne peut dépasser 100 000 francs, le montant pour ces cas de faible importance (cas dit «bagatelle») a été fixé à 20 000 francs.

65 FF **2017** 6565 p. 6603 et 6718
66 RS **313.0**

Si l'on pense que l'obligation de signaler se concentre sur les principales infrastructures critiques, lesquelles peuvent bien souvent prétendre à une part de marché significative, aucun argument ne justifie de fixer le montant maximal de 20 000 francs à un niveau plus bas.

Il n'existe également aucune possibilité de fixer l'amende à un niveau plus élevé pour les entreprises, par exemple en pourcentage du chiffre d'affaires. Dans le droit suisse, la punissabilité de l'entreprise est toujours subsidiaire à celle des personnes physiques (cf. en particulier art. 29 et 102 CP), raison pour laquelle l'imputation de l'amende à l'entreprise n'est possible que pour les cas de faible importance.

Al. 4

Pour des raisons de transparence, l'al. 4 mentionne, par analogie à l'art. 65 nLPD, la compétence des autorités cantonales de poursuite pénale au cas où une décision du NCSC ne serait pas suivie d'effet. Il a été décidé de ne pas mentionner le droit de dénonciation du NCSC, car cette circonstance découle du contexte.

Section 3: Protection des données et échange d'informations

Les art. 75 à 79, qui sont désormais regroupés dans la section 3, ont dû être adaptés tant sur le plan linguistique que sur le plan du contenu afin de correspondre à l'ancrage légal des tâches du NCSC. Avec son guichet de signalement, le NCSC remplace MELANI, qui était exploité conjointement par l'ancienne Unité de pilotage informatique de la Confédération (UPIC) et le SRC. Comme le SRC a un mandat légal d'évaluation de la menace et d'alerte précoce des exploitants d'infrastructures critiques, la collaboration du NCSC avec le SRC et la transmission d'informations et de données doivent, dans la mesure nécessaire, être réglées dans la LSI.

Art. 75 Traitement des données personnelles

La portée matérielle de l'art. 75 a été étendue lors de la révision du chapitre 5 afin que le NCSC dispose d'une base légale pour traiter des données personnelles, même lorsque celles-ci n'ont aucun lien avec les ressources d'adressage. Plusieurs adaptations de nature systématique et formelle y ont également été apportées, par exemple l'ajout de la désignation «NCSC».

Al. 1

En lieu et place d'une description générique des services fédéraux compétents, le NCSC a été ajouté et l'al. 1 a été fusionné avec l'al. 2. Comme dans le droit en vigueur, il est possible de traiter non seulement des données personnelles, mais également des données sensibles qui se rapportent aux ressources d'adressage. Selon la définition donnée à l'art. 3, let. f, LTC, une ressource d'adressage est «la suite de chiffres, de lettres ou de signes ou toute autre information permettant d'identifier une personne, un processus informatique, une machine, un appareil ou une installation de télécommunication qui intervient dans une opération de télécommunication».

Aux let. a et b, le verbe a été supprimé dans la version allemande. Le terme «cybersécurité» a été ajouté à la let. a. Les explications relatives aux données sensibles selon

les let. a et b ont été fournies dans le message du 22 février 2017 concernant la loi sur la sécurité de l'information[67] et ne sont donc pas répétées ici.

Al. 2

L'al. 2 reprend pour l'essentiel les anciens al. 3 et 4, la formulation ayant été transformée à la voix active dans la version allemande pour montrer plus clairement que le traitement des données est effectué par le NCSC. En outre, les conditions qui doivent être remplies pour que le NCSC n'informe pas la personne concernée du traitement des données ou de l'usurpation d'identité ont été précisées.

Art. 76 Collaboration sur le plan national

Cet article constitue la base légale de l'échange d'informations entre le NCSC et les exploitants d'infrastructures critiques (al. 1 et 2) ainsi qu'entre le NCSC et les fournisseurs de services de télécommunication (al. 3 et 4), lorsque ceux-ci ne sont pas qualifiés d'infrastructures critiques.

Sur le plan matériel, l'art. 76 correspond largement à la version adoptée par le Parlement le 18 décembre 2020. Outre quelques adaptations linguistiques (par ex. l'ajout des termes «cybermenaces» et «NCSC»), cette disposition a subi quelques changements d'ordre systématique: les al. 1 et 2 définissent l'échange d'informations entre le NCSC et les exploitants d'infrastructures critiques et les al. 3 et 4 (nouveaux), l'échange d'informations entre le NCSC et les fournisseurs de services de télécommunication.

Al. 1 et 2

L'échange d'informations entre le NCSC et les exploitants d'infrastructures critiques, qui est réglé aux al. 1 et 2, ne se limite pas aux infrastructures critiques assujetties à l'obligation de signaler, mais est ouvert à toutes les infrastructures critiques intéressées ayant leur siège en Suisse. Cela veut dire que l'échange d'informations n'est pas réservé aux assujettis à l'obligation de signaler en vertu de l'art. 74*b* et que les infrastructures critiques exemptées de l'obligation de signaler conformément à l'art. 74*c* peuvent aussi y prendre part.

Aux fins de l'échange d'informations avec les infrastructures critiques, qui doit s'effectuer par un canal de communication sécurisé, le NCSC utilise le protocole TLP (Traffic Light Protocol), qui prévoit une répartition internationalement reconnue des informations confidentielles en quatre catégories, en vue de leur utilisation et de leur éventuelle transmission.

La portée de l'échange d'informations entre le NCSC et les infrastructures critiques a été élargie par rapport à la version initiale, car la limitation aux ressources d'adressage et aux données sensibles qui s'y rapportent n'était pas appropriée. Pour l'alerte précoce et pour la défense contre des cyberattaques imminentes, le NCSC a besoin que les infrastructures critiques lui communiquent aussi des données personnelles qui ne se rapportent pas à des ressources d'adressage. Les infrastructures critiques doivent être autorisées à communiquer au NCSC des données personnelles qui ne sont pas en

67 FF **2017** 2765 p. 2870 ss

lien direct avec un cyberincident (comme cela était prévu initialement à l'al. 3), mais qui ont, par exemple, un rapport avec des cybermenaces. Ce complément est conforme au message concernant la loi sur la sécurité de l'information, dans lequel il était précisé que les infrastructures critiques communiquent les «informations liées à des dangers et des incidents» à MELANI et que, «dans le but de prévenir des dangers et d'éviter des préjudices, [elles] peuvent fournir des indications sur les services qu'[elles] fournissent, leurs activités d'intermédiaire et d'autres opérations»[68]. Il a été décidé de profiter de la présente révision du chapitre 5 pour préciser le libellé de la loi, afin de s'assurer que le NCSC puisse échanger avec les infrastructures critiques toutes les informations, y compris les données personnelles, qui sont nécessaires pour l'alerte précoce et la protection contre les cybermenaces.

Al. 3 et 4

L'échange d'informations entre le NCSC et les fournisseurs de services de télécommunication a été explicitement réglé aux al. 3 et 4, car si la plupart de ces fournisseurs sont considérés comme des infrastructures critiques, ce n'est probablement pas le cas de tous.

La deuxième phrase de la version initiale de l'al. 3, qui prévoit que MELANI ne peut transmettre des données à des fins de poursuite pénale qu'avec le consentement exprès du fournisseur de données, a été biffée. Cette norme est devenue inutile avec la création d'un droit de dénoncer pour le directeur du NCSC (art. 73*d*, al. 3).

Art. 76a Soutien aux autorités

Cette disposition est nouvelle. Elle règle les informations que le NCSC met à la disposition d'autres autorités, dans quelle mesure et à quelles fins. Elle clarifie la répartition des rôles entre le NCSC et le SRC (al. 1) ainsi que le contenu et les modalités de la communication des informations au SRC, aux autorités de poursuite pénale et aux services cantonaux responsables de la cybersécurité (al. 2 à 4).

Un des aspects importants de la collaboration du NCSC avec ces autorités concerne les informations recueillies par le NCSC sur les auteurs de cyberattaques et sur les méthodes et tactiques qu'ils utilisent. Seules ces informations sont communiquées aux autres autorités.

Al. 1

L'al. 1 établit que le NCSC apporte son soutien au SRC dans ses tâches en lui fournissant des évaluations spécifiques du nombre, du type et de l'ampleur des cyberattaques ainsi que des analyses techniques des cybermenaces. Ces tableaux de situation ne contiennent pas de données personnelles ou d'informations concrètes et spécifiques à chaque cas, mais se limitent aux évaluations statistiques et techniques nécessaires à l'évaluation de la menace et à l'alerte précoce. En vertu de l'art. 6, al. 2, LRens, le SRC a pour tâche d'apprécier la menace. Or le NCSC dispose, avec son guichet de signalement – et avec les signalements supplémentaires qu'il recevra en exécution de l'obligation de signaler –, de sources d'information importantes sur l'état de la menace liée aux cyberincidents. Il peut donc fournir au SRC des informations sur le

68 FF **2017** 2765 p 2872 s.

nombre, le type et l'ampleur des cyberattaques, et lui apporter son soutien avec des analyses techniques sur les attaques et des évaluations des résultats de ces analyses.

Al. 2, 3 et 4

Les al. 2 à 4 règlent le contenu, l'étendue et les modalités de l'échange d'informations du NCSC avec le SRC, les autorités de poursuite pénale et les services cantonaux chargés de la cybersécurité.

D'un point de vue matériel, le soutien du NCSC consiste à donner accès à ces autorités aux informations sur les auteurs de cyberattaques et sur les méthodes et tactiques qu'ils utilisent. Ces informations peuvent être de nature purement technique (par ex. mode opératoire ou valeurs de hachage des maliciels) et ne pas renfermer de données personnelles. Mais ces autorités échangent également entre elles des informations personnelles ou permettant d'établir un lien avec des personnes données. Concrètement, il s'agit de ressources d'adressage (comme le nom de domaine, l'adresse IP ou les adresses de messagerie utilisées de manière abusive) ou d'indications sur des transactions financières (comptes bancaires, numéros IBAN, etc.). Aussi une base légale est-elle créée ici pour les échanges d'informations se rapportant à ces données personnelles.

Les autorités habilitées à le faire en vertu des al. 2 à 4 peuvent accéder aux informations susmentionnées de manière autonome. Cette approche est judicieuse en raison du grand nombre de cyberattaques et d'informations techniques associées, afin de permettre la comparaison des informations dans les meilleurs délais possibles.

Le NCSC ne communique qu'exceptionnellement d'autres informations obtenues dans le cadre du signalement des cyberattaques et uniquement aux conditions prévues à l'art. 73*c*.

Art. 77 Coopération internationale

Cette disposition ne connaît que des modifications formelles par rapport à la version initiale. Désormais, le NCSC est cité par son nom et le terme de «données» a été remplacé par le terme générique d'«informations». En outre, le champ d'activité des services étrangers a été précisé: ces derniers ne doivent plus être chargés de la «protection d'infrastructures critiques» (version initiale), mais de la «cybersécurité». L'ancien libellé n'était pas assez spécifique et aurait pu entraver le bon déroulement des échanges d'informations avec d'importantes organisations internationales actives dans le secteur de la cybersécurité.

Al. 1 et 2

Le contenu des informations que le NCSC peut communiquer à ces organisations se limite à l'identité et au mode opératoire des auteurs de cyberattaques. La portée est donc la même que pour le soutien aux autorités conformément à l'art. 76*a*. Il va de soi que le NCSC communique les informations dans le respect du droit de la protection des données.

Les organisations de cybersécurité étrangères ou internationales doivent utiliser les informations du NCSC concernant les caractéristiques des cyberattaques et les méthodes déployées de manière conforme à leur destination. Le NCSC s'en assure grâce

à l'utilisation du protocole TLP, qui catégorise les informations confidentielles selon un modèle internationalement reconnu et détermine pour chaque niveau de protection les conditions d'utilisation et de transmission des informations.

La nLPD sera déjà applicable lorsque le présent projet entrera lui-même en vigueur, raison pour laquelle l'al. 1 renvoie déjà à celle-ci.

Al. 3

La réserve relative à l'assistance administrative et à l'entraide judiciaire prévue à l'al. 3 est biffée.

Avec la création de l'obligation de signaler, tout le contexte du chapitre 5 a changé et la confidentialité du traitement des signalements par le NCSC a encore gagné en importance. De fait, les signalements au NCSC et leur analyse, pour autant qu'ils reposent sur des informations de tiers, ont été exclus du champ d'application de la LTrans (art. 4, al. 1bis). Pour la même raison, l'obligation de dénoncer les infractions qui incombe au personnel du guichet de signalement a été restreinte au seul directeur du NCSC. Il existe certes un droit de transmettre les informations en rapport avec les cyberincidents signalés, mais seulement dans des cas exceptionnels et pour autant que lesdites informations soient particulièrement pertinentes sur le plan sécuritaire ou pénal (art. 73*d*).

Dans cette perspective, la réserve relative à l'assistance administrative et à l'entraide judiciaire pourrait être mal interprétée. Le NCSC ne peut fournir l'assistance administrative que si cela est prévu par une disposition du droit matériel. Mais même dans ce cas, il ne peut divulguer des informations que si aucune disposition protégeant la confidentialité des données ne s'y oppose. Dans les faits, le NCSC ne pourra donc fournir l'assistance administrative que dans de rares cas.

Art. 78 Système d'information pour le soutien aux infrastructures critiques

Cet article a été rendu superflu par la révision de la LPD et il est donc abrogé.

Les buts du traitement des données par le NCSC découlent de ses tâches, lesquelles sont décrites avec une précision suffisante dans les articles consacrés à la question. Ils fixent déjà ce qui peut être fait avec les systèmes d'information du NCSC lors du traitement des données personnelles.

Art. 79 Conservation et archivage des données

L'al. 1 est reformulé d'une manière plus restrictive que la version initiale adoptée par le Parlement[69].

On y précise que les données personnelles peuvent être conservées pendant cinq ans au plus à compter de la dernière fois où elles ont été utilisées pour détecter des cybermenaces ou gérer des cyberincidents. Cette réglementation tient au fait que certaines informations techniques sur les cyberincidents, à l'instar du nom de domaine, de l'adresse IP ou des adresses de messagerie utilisées de manière abusive, revêtent une

69 «Les services visés à l'art. 74, al. 5, conservent les données personnelles aussi longtemps que celles-ci sont utiles pour prévenir des dangers ou pour identifier des incidents, mais cinq ans au plus» (art. 79, al. 1, version du 18 décembre 2020).

importance centrale lors des comparaisons entre les cyberincidents nouvellement signalés et l'analyse des méthodes d'attaque ou des modes opératoires. Faute de telles données de comparaison, le NCSC ne pourrait pas effectuer – ou du moins pas de manière ciblée – ses analyses, qui constituent une condition essentielle de l'accomplissement de ses tâches.

Même en cas de non-utilisation prolongée, les données doivent pouvoir être interrogées par le NCSC à des fins de comparaison. Le message concernant la loi sur la sécurité de l'information relevait à ce propos que «les vecteurs d'attaque peuvent rester utiles de longues années».[70] Mais comme ces données techniques renferment aussi des éléments à caractère personnel et, à ce titre, sont soumises à la protection des données en tant que données personnelles – et que leur anonymisation entraverait considérablement ou empêcherait même l'accomplissement des tâches du NCSC –, leur durée de conservation a été clairement délimitée en prenant leur dernière utilisation comme point de référence.

Pour des raisons tenant à la protection des données, il a été ajouté dans la deuxième partie de la phrase que les données sensibles peuvent être conservées au maximum deux ans à compter de leur dernière utilisation. Cette précision ne figurait pas dans la version initiale.

Art. 80 Dispositions édictées par le Conseil fédéral

Cet article est abrogé.

La compétence d'édicter des dispositions d'exécution revient au Conseil fédéral, même sans réserve de la loi (ch. 4.3.3).

Loi fédérale du 21 juin 2019 sur les marchés publics[71]

Dans le cadre de la procédure de consultation relative à l'avant-projet, il a été suggéré[72] que, lorsque des fabricants de matériel informatique et de logiciels n'éliminent pas une vulnérabilité dans le délai qui leur a été imparti, ceux-ci soient tenus de répondre de leur manquement dans le cadre du droit des marchés publics.

Outre l'intérêt public à ne pas mettre en péril la cybersécurité par des vulnérabilités, il existe aussi un intérêt public à exclure les fabricants défaillants des marchés publics. Le droit actuel permet déjà d'exclure les produits proposés lorsqu'ils comportent des vulnérabilités non éliminées. Les produits en question, qui ne répondent pas (ou plus) aux exigences en raison de ces vulnérabilités, présentent un vice et ne remplissent donc pas (ou plus) les spécifications techniques si le vice a une importance significative dans l'optique du but prévu ou prévisible. Or les spécifications techniques et les normes courantes doivent impérativement être remplies en tout temps, de sorte que les offres concernées peuvent être exclues en vertu de l'art. 44, al. 1, let. a ou b, LMP[73].

70 FF **2017** 2765 p. 2874
71 RS **172.056.1**
72 Cf. avis de CH++.
73 Cf. Handkommentar zum Schweizerischen Beschaffungsrecht, Trüeb (éd.), Locher ad Art. 44, ch. 12 et 13.

Il est toutefois nécessaire de prévoir une possibilité d'exclusion en tant que conséquence directe du comportement non coopératif d'un fabricant dans le cadre de la procédure de divulgation coordonnée des vulnérabilités (*coordinated vulnerability disclosure*). Ce n'est en effet que si les fabricants s'engagent réellement à éliminer les vulnérabilités qu'il est judicieux de les informer d'abord à ce sujet.

L'ajout d'une let. f^{bis} à la liste des critères prévue à l'art. 44, al. 1, instaure la possibilité d'exclure des soumissionnaires de futurs marchés ou de résilier des contrats en cours, comme conséquence directe de leur manque de coopération dans le processus de résolution des vulnérabilités.

Pour pouvoir être informés en temps utile sur les vulnérabilités du matériel informatique et des logiciels qui ne sont pas encore résolues, les services d'achat centraux, les responsables de la sécurité informatique et les responsables de la gestion des contrats peuvent participer à l'échange d'informations du NCSC avec les infrastructures critiques.

Il convient enfin de relever que cette nouvelle disposition de la LMP ne déploie ses effets qu'au niveau fédéral et qu'elle va ainsi à l'opposé de l'objectif principal de la récente révision totale de la LMP, qui était l'harmonisation de cette loi avec l'accord intercantonal sur les marchés publics (AIMP 2019).

Modification du 25 septembre 2020 de la loi sur la protection des données[74]

Afin que le PFPDT puisse faire appel aux spécialistes techniques du NCSC lors de l'analyse d'une violation de la sécurité des données que le responsable lui a signalée en vertu de l'art. 24 nLPD et de l'art. 19 OLPD, l'art. 24, al. 5bis, nLPD prévoit que le PFPDT peut transmettre au NCSC le signalement d'une violation de la sécurité des données.

La transmission peut contenir toutes les indications prévues à l'art. 19, al. 1, OLPD, mais doit en même temps se limiter aux données nécessaires au NCSC pour qu'il analyse l'incident. L'annonce transmise par le PFPDT au NCSC peut également renfermer des données personnelles, y compris des données sensibles relatives à des poursuites ou à des sanctions administratives et pénales visant le responsable du traitement. Les informations nécessaires en vue de l'analyse d'un incident sont sélectionnées dans chaque cas d'espèce, mais, dans certaines circonstances, des informations concernant une procédure en cours peuvent très bien parvenir indirectement au NCSC. Il faut par conséquent créer une base légale régissant la divulgation de données sensibles.

La condition est ici que le responsable tenu d'informer le PFPDT ait donné son consentement préalable à la transmission de l'annonce. En outre, la transmission ne doit pas conduire à éluder l'art. 24, al. 6, nLPD, selon lequel l'annonce ne peut être utilisée dans le cadre d'une procédure pénale contre la personne tenue d'annoncer qu'avec son consentement. Cela veut dire qu'un responsable pourra toujours se prévaloir de l'interdiction d'utiliser les données en tant que preuves en vertu du droit de la protection des données, même en cas de transmission de son annonce au NCSC. À

74 RS **235.1**; RO **2022** 491

l'art. 24 nLPD, le nouvel al. 5bis ne permet pas au PFPDT de transmettre systématiquement les signalements au NCSC. Au contraire, il ne peut faire usage de cette possibilité que dans les cas où il a besoin de l'expertise technique du NCSC pour élucider les circonstances d'un incident.

Ce droit de transmission d'informations du PFPDT au NCSC se limite à un échange d'informations unilatéral. Pour sa part, le NCSC ne fournit aucune information provenant des signalements au PFPDT, même lorsque ceux-ci comportent des violations de la protection des données. Le NCSC met toutefois à la disposition des auteurs de signalements un système électronique qui leur permet de communiquer leur signalement en tout ou en partie. L'auteur d'un signalement a donc la possibilité d'utiliser le formulaire de signalement d'une cyberattaque pour signaler une violation de la protection des données au PFPDT.

La loi révisée sur la protection des données devrait entrer en vigueur en septembre 2023, soit peu après l'entrée en vigueur de la LSI (dans sa version antérieure au présent projet). À partir de là et jusqu'à l'entrée en vigueur du chapitre 5 révisé de la LSI (le présent projet) – au plus tôt fin 2023 – la réglementation prévue à l'art. 24, al. 5bis, s'appliquera déjà au niveau de l'ordonnance (art. 41, al. 1, de l'ordonnance du 31 août 2022 sur la protection des données)[75]. Le Conseil fédéral abrogera cette disposition de l'ordonnance dès l'entrée en vigueur du présent projet.

Loi du 21 mars 2003 sur l'énergie nucléaire[76]

Le nouvel art. 102, al. 2, LENu crée une base légale explicite pour que l'IFSN, en sa qualité de guichet de signalement sectoriel, transmette au guichet de signalement intersectoriel du NCSC les signalements de cyberattaques contre les installations nucléaires, lorsqu'elles remplissent les conditions posées à l'art. 74*d* LSI. Cela permettra au NCSC de recevoir les signalements concernant les cyberattaques sans interférer dans les processus qui ont été mis en place pour les installations nucléaires.

Loi du 23 mars 2007 sur l'approvisionnement en électricité[77] *(LApEl)*

Une étude réalisée pour le compte de l'Office fédéral de l'énergie a mis en évidence un besoin de réglementation important en matière de cybersécurité dans ce domaine primordial pour l'approvisionnement économique et pour la sécurité du pays qu'est l'approvisionnement en électricité.[78] Les conclusions de cette étude montrent que les directives sectorielles subsidiaires qui ont été mises en place au fil du temps ne se sont pas traduites par une protection adéquate contre les cybermenaces. La protection contre les cybermenaces, qui figurera désormais explicitement à l'art. 8*a* LApEl, contribue à la sécurité de l'approvisionnement.

Les mesures visées à l'al. 1 doivent permettre soit de prévenir, soit de régler au plus vite les cyberincidents et donc, en particulier, les dysfonctionnements des installations

75 RS **235.11**; RO **2022** 568
76 RS **732.1**
77 RS **734.7**
78 Rapport du 28 juin 2021 Stratégie de cybersécurité pour l'approvisionnement suisse en électricité: www.bfe.admin.ch > Approvisionnement > Approvisionnement en électricité: La numérisation du monde de l'énergie (disponible en allemand uniquement)

concernées. Outre les gestionnaires de réseau qui interviennent directement dans l'exploitation au moyen de technologies de pilotage, l'obligation vaut aussi pour les producteurs (par ex. les exploitants d'éoliennes ou de centrales hydro-électriques) et pour les agents de stockage, d'autant plus qu'ils peuvent exercer une influence majeure sur la sécurité de l'approvisionnement par leurs activités d'injection et de prélèvement de courant. Pour juger du degré de protection adéquat, il faut examiner l'influence que l'opérateur en question peut avoir sur la sécurité de l'approvisionnement (par ex. niveau du réseau, puissance connectée, puissance installée, nombre de consommateurs finaux concernés).

La surveillance du respect de l'art. 8*a* incombe à la Commission fédérale de l'électricité (ElCom) en vertu de sa compétence générale subsidiaire (art. 22, al. 1, LApEl). Le Conseil fédéral édictera les dispositions d'exécution correspondantes, notamment en ce qui concerne le niveau de protection visé et les audits à effectuer (par ex. obligation de fournir des documents à l'ElCom). En vertu du principe de subsidiarité (art. 3, al. 2, LApEl), il s'appuiera pour cela sur les directives sectorielles pertinentes (par ex. le manuel de l'Association du secteur électrique suisse AES Protection de base pour les «technologies opérationnelles» [OT] dans l'approvisionnement en électricité, édition de juillet 2018, en cours de révision), qu'il pourra également déclarer contraignantes.

L'al. 2 permet au Conseil fédéral d'assujettir certains prestataires de l'approvisionnement en électricité à l'obligation prévue à l'al. 1, par exemple dans les domaines du commerce et de la mesure de l'énergie, du pilotage, de la flexibilité, du traitement des données ou de la mobilité électrique. Compte tenu de la finalité de cette disposition, seuls sont visés les opérateurs qui exercent une influence déterminante sur la sécurité de l'approvisionnement. Tel est le cas lorsque, dans le cadre de leurs activités, ils peuvent accéder aux systèmes de gestion d'un grand nombre d'entreprises d'approvisionnement en électricité, de sorte qu'un grand nombre de consommateurs finaux seraient concernés, ou lorsque prestataires actifs dans les secteurs de la mobilité électrique ou de la production décentralisée gèrent, par agrégation, une puissance importante dans le système d'approvisionnement en énergie.

En se fondant sur l'al. 2, le Conseil fédéral peut aussi prévoir des exceptions, par exemple pour les exploitants de réseaux de distribution comptant peu de consommateurs finaux ou pour les producteurs qui ont une faible puissance installée. D'autres exceptions peuvent être envisagées, par exemple pour les entreprises qui doivent déjà prendre des mesures particulières dans le domaine de la cybersécurité en vertu de la législation spéciale (par ex. dans le secteur du courant de traction ferroviaire). Une coordination sera nécessaire au niveau des ordonnances.

Loi du 22 juin 2007 sur la surveillance des marchés financiers (LFINMA).[79]

Le secteur des marchés financiers connaît lui aussi une obligation de signaler les cyberattaques. Les signalements en question doivent être adressés à la FINMA. Étant donné que, en cas de cyberattaque, les acteurs des marchés financiers sont déjà soumis à une autre obligation de signaler, le NCSC aménagera son système de signalement

79 RS **956.1**

électronique de manière à ce que les auteurs des signalements puissent utiliser le formulaire du NCSC pour s'acquitter simultanément de leurs obligations à l'égard de la FINMA.

Indépendamment de cela, la FINMA doit, lors d'une cyberattaque, être autorisée à communiquer au NCSC les informations non accessibles au public dont le NCSC a besoin pour s'acquitter de ses tâches. À cet effet, le NCSC est ajouté à l'énumération contenue à l'art. 39, al. 1, LFINMA, ce qui crée la base légale nécessaire pour que la FINMA puisse communiquer des informations à cet organe.

6 Conséquences

6.1 Conséquences pour la Confédération

Le NCSC gère déjà à l'heure actuelle un service d'alerte qui recueille les signalements de cyberincidents effectués sur une base volontaire. Il bénéficie en la matière de la longue expérience de MELANI, qui se chargeait déjà de cette tâche depuis 2004 pour les annonces spécifiques aux infrastructures critiques.

6.1.1 Conséquences financières

Le NCSC utilise déjà aujourd'hui un formulaire électronique pour la collecte des signalements. Il serait possible de l'adapter afin qu'il puisse aussi servir à la réception des signalements faisant suite à l'obligation de signaler. Un investissement initial sera certes indispensable en vue de l'harmonisation nécessaire avec les autres services collectant des signalements (par ex. PFPDT, FINMA, IFSN) et de la configuration du formulaire de signalement, mais il sera gérable avec les ressources dont dispose le NCSC. Celui-ci devra toutefois s'assurer, au stade de l'exploitation, que les signalements faisant suite à l'obligation de signaler soient correctement enregistrés, qu'ils fassent l'objet d'un accusé de réception, qu'ils soient dûment documentés et, enfin, qu'ils soient transmis aux services compétents à des fins de détection précoce. Ce surcroît de travail devra être pris en compte lors des développements futurs du NCSC.

6.1.2 Conséquences sur l'état du personnel

Après une cyberattaque, le NCSC aide l'exploitant de l'infrastructure critique concernée à gérer l'incident. Cette prestation de soutien fonctionne déjà bien, grâce à la longue expérience du NCSC (et, auparavant, celle de MELANI). Il faut toutefois s'attendre à ce que la charge de travail du NCSC augmente suite à l'introduction de l'obligation de signaler. Outre que les signalements seront plus nombreux, le NCSC devra procéder à une première évaluation et émettre les recommandations utiles pour gérer l'incident. Il faudra dès lors étoffer son équipe chargée des analyses techniques (GovCERT). Les charges de personnel supplémentaires qui en découlent ne peuvent pas encore être estimées avec une précision suffisante et leur évaluation ne peut pas se faire sans tenir compte de l'orientation future de la stratégie nationale de protection de la Suisse contre les cyberrisques et de l'organisation du NCSC, qui sont examinées par le Conseil fédéral en ce moment. Ces charges supplémentaires seront déterminées avant l'adoption des dispositions d'exécution et feront alors l'objet d'une demande en bonne et due forme.

6.2 Conséquences pour les cantons et les communes, ainsi que pour les centres urbains, les agglomérations et les régions de montagne

Ce projet n'attribue pas de nouvelles tâches aux cantons et aux communes, mais ceux-ci sont concernés par l'obligation de signaler pour deux raisons: premièrement, les autorités cantonales et communales sont elles-mêmes assujetties à l'obligation de signaler en vertu de l'art. 74*b*, let. b, et deuxièmement, des organismes cantonaux ou communaux sont responsables de nombreuses entreprises assujetties à cette obligation.

En contrepartie, les cantons et les communes profitent également des prestations du NCSC pour mieux se protéger contre les cybermenaces. Aujourd'hui déjà, beaucoup de cantons et de villes participent aux échanges d'informations entre infrastructures critiques et sont intégrés au NCSC.

6.3 Conséquences pour l'économie, la société et l'environnement

Il ne devrait y avoir aucune conséquence directe pour l'économie, la société et l'environnement. L'économie et la société profiteront indirectement de l'introduction d'une obligation de signaler les cyberattaques, étant donné que l'amélioration de la cybersécurité des infrastructures critiques sera positive pour la cybersécurité de tout le pays. Par ailleurs, l'obligation de signaler contribuera à éviter, grâce à des mesures de prévention et de défense précoces, que des cyberattaques lancées contre des infrastructures critiques n'entraînent des perturbations ou des pannes de services essentiels, mettant en péril le bon fonctionnement de l'économie et de l'État.

L'introduction d'une obligation de signaler les cyberattaques subies par les infrastructures critiques n'aura aucun impact pour l'économie ou les entreprises concernées, ou du moins ses conséquences resteront négligeables. Il n'est dès lors pas nécessaire de procéder à une analyse d'impact de la réglementation.

L'obligation de signaler aide à assurer la transparence sur la menace liée aux cyberattaques et contribue à sensibiliser la population aux cybermenaces. Des cybercompétences accrues au sein de la population sont la condition essentielle d'une fructueuse transformation numérique de la société.

7 Aspects juridiques

7.1 Constitutionnalité

La Constitution fédérale ne contient pas de bases juridiques explicites permettant d'introduire une obligation de signaler les cyberattaques. Pour introduire une obligation de signaler les cyberattaques visant des infrastructures critiques, la Confédération peut s'appuyer sur sa compétence fédérale inhérente en matière de préservation de la sécurité intérieure et extérieure de la Confédération.

Pour leur sécurité, la société, l'économie et l'État dépendent largement des infrastructures critiques. De par leurs conséquences potentiellement graves à l'échelle nationale, les cyberattaques dirigées contre les infrastructures critiques menacent la prospérité du pays et risquent de compromettre sa sécurité tant intérieure qu'extérieure. L'introduction d'une obligation de signaler aide donc à préserver la stabilité économique, sociale et étatique du pays. Elle constitue la base de la coordination et de la rapidité de la gestion des événements. L'obligation de signaler les cyberattaques contre les infrastructures critiques permet en outre d'établir, à partir des signalements, une analyse du niveau de menace à des fins d'alerte précoce et de prévention des dangers. Il ressort de l'objectif de cette obligation que son champ d'application doit être limité aux cyberattaques visant des infrastructures critiques. Le droit de signaler les cyberincidents et les vulnérabilités, ouvert à tous, permet à titre complémentaire la collecte d'informations supplémentaires en vue de protéger les infrastructures critiques.

En conséquence, la compétence dévolue à la Confédération de préserver la sécurité intérieure et extérieure – avec des compétences qui, sans lui être expressément accordées, lui reviennent en tant qu'État – constitue une base constitutionnelle adéquate pour l'édiction de dispositions législatives relatives à une obligation de signaler les cyberattaques et à un droit de signaler les cyberincidents et les vulnérabilités.

En vertu d'une convention formelle de technique législative[80], l'art. 173, al. 2, Cst. est généralement cité comme base juridique pour les compétences inhérentes de la Confédération sans base constitutionnelle explicite. Étant donné que le préambule de la LSI mentionne déjà (outre les art. 54, al. 1, 60, al. 1, 101, 102, al. 1, et 173, al. 1, let. a et b) l'art. 173, al. 2, comme base juridique déterminante, il n'est pas nécessaire de le compléter.

7.2 Compatibilité avec les obligations internationales de la Suisse

L'introduction d'une obligation de signaler les cyberattaques ne contrevient à aucune obligation internationale de la Suisse. Elle est comparable aux réglementations introduites au cours des dernières années par bien d'autres États, dont en particulier les États membres de l'UE.

7.3 Forme de l'acte à adopter

Le choix de compléter la LSI déjà adoptée pour en faire la base légale nécessaire à l'introduction de l'obligation de signalement semble idéal. Outre que le but, l'objet et le champ d'application de la LSI sont compatibles avec l'obligation de signaler faite aux infrastructures critiques, elle constitue la base légale formelle du NCSC en tant que guichet de signalement. D'un point de vue systématique, l'obligation de signaler les cyberattaques ainsi que les tâches de protection de la cybersécurité incombant au NCSC peuvent être introduites au chapitre 5.

80 Directives de la Confédération sur la technique législative, ch. 25. Consultable en ligne sous: www.chf.admin.ch > Documentation > Accompagnement législatif > Directives sur la technique législative DTL

Il faudra encore décider, à propos des dispositions d'exécution relatives à l'obligation de signalement, si cette obligation doit faire l'objet d'une ordonnance à part entière ou s'il convient de compléter des ordonnances en vigueur.

7.4 Frein aux dépenses

Le projet ne contient pas de dispositions relatives aux subventions et ne prévoit ni crédits d'engagement, ni plafonds de dépenses (qui entraîneraient des dépenses supérieures à l'un des seuils définis par la loi).

7.5 Conformité aux principes de subsidiarité et d'équivalence fiscale

L'attribution et l'accomplissement de tâches étatiques se fondent sur le principe de subsidiarité (art. 5*a* Cst.). Conformément à l'art. 43*a*, al. 1, Cst., la Confédération n'assume que les tâches qui excèdent les possibilités des cantons ou qui nécessitent une réglementation uniforme par la Confédération. Simultanément, la Confédération doit faire un usage modéré de ses compétences et laisser suffisamment de latitude aux cantons dans l'accomplissement de leurs tâches.

Une obligation de signaler les cyberattaques ne peut être mise en œuvre de manière efficace qu'à condition de s'étendre à tout le territoire suisse et à tous les secteurs d'activités. Sans procédure de signalement uniforme ni guichet de signalement centralisé, il sera impossible de venir à bout de cyberattaques déployées au-delà des frontières cantonales et des domaines de spécialisation. En vertu de la compétence dévolue à la Confédération, cette obligation a été limitée aux cyberattaques subies par les infrastructures critiques, dont l'impact constitue une menace pour la sécurité nationale et le bon fonctionnement de l'État. L'introduction de l'obligation de signaler constitue par conséquent une mesure conciliable avec le principe de subsidiarité (art. 5a en relation avec l'art. 43*a* Cst.).

Selon le principe d'équivalence fiscale établi à l'art. 43*a*, al. 2 et 3, Cst., toute collectivité bénéficiant d'une prestation de l'État prend en charge les coûts de cette prestation et toute collectivité qui prend en charge les coûts d'une prestation de l'État décide de cette prestation. Ce principe est respecté dans le cadre de l'introduction de l'obligation de signaler, étant donné que la Confédération couvrira les coûts d'exploitation du guichet d'enregistrement. Pour les infrastructures critiques, cette obligation ne change pas grand-chose: elles pourront compter, comme jusqu'ici, sur le soutien du NCSC pour la gestion des incidents. L'obligation de signaler n'entraînera qu'un léger surcroît de travail par rapport aux signalements de cyberincidents effectués sur une base volontaire. Par conséquent, il n'y aura pas de véritables coûts supplémentaires, même dans le cas des infrastructures critiques exploitées par les cantons ou les communes.

7.6 Délégation de compétences législatives

Selon le présent projet, les éléments centraux pour l'introduction de l'obligation de signaler les cyberincidents doivent être inscrits dans la loi.

Si nécessaire, le Conseil fédéral édictera des dispositions d'exécution pour concrétiser les dispositions légales. Il lui incombe notamment, en vertu de l'art. 74*c*, de restreindre

davantage le cercle des assujettis à l'obligation de signaler. La loi définit les critères à appliquer à cet effet, mais il appartiendra au Conseil fédéral de déterminer pour chaque secteur quels critères seront appliqués et comment (par ex. en définissant des valeurs seuils appropriées).

7.7 Protection des données et principe de transparence

Le projet mis en consultation a pratiquement repris telles quelles les exigences en matière de protection des données que le Parlement avait initialement adoptées au chapitre 5 de la LSI, dans le contexte du soutien apporté par la Confédération aux exploitants d'infrastructures critiques.

Une nouvelle disposition a été introduite dans la LSI (art. 4, al. 1bis) afin que les informations de tiers qui ont été transmises au NCSC dans le cadre de l'obligation de signaler ou dont celui-ci a pris connaissance en analysant de tels signalements ne puissent pas être rendues accessibles en vertu de la loi sur la transparence.

Le PFPDT est opposé à cette disposition. Il estime que cette exception violerait le principe de transparence en empêchant les citoyens d'avoir accès à des informations qui sont en relation directe avec l'accomplissement d'une tâche centrale du NCSC, ce qui entraverait le contrôle public dans un domaine sensible. De plus, le PFPDT relève que la multitude d'exceptions prévues par la LTrans est suffisante pour protéger les différents intérêts en présence et que l'introduction d'une nouvelle exception est donc superflue. Le PFPDT ne voit pas en quoi l'application de la LTrans pourrait entraver l'activité du NCSC dans sa fonction de guichet de signalement.

Annexes (projets d'actes législatifs)