Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Centre national pour la cybersécurité NCSC

Berne, le 12 janvier 2022

Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques

Modification de la loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (loi sur la sécurité de l'information, LSI)

Rapport explicatif
relatif à l'ouverture de la procédure de consultation

Table des matières

Condensé

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 projet mis en consultation prévoit d'introduire une obligation de signaler les cyberattaques contre les infrastructures critiques. Une telle obligation permettra de détecter précocement les cyberattaques, d'analyser leur mode opératoire 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 11 décembre 2020, le Conseil fédéral a chargé le Département fédéral des finances (DFF) d'élaborer un projet fournissant les bases légales nécessaires à l'introduction d'une obligation de signaler les cyberattaques contre les infrastructures critiques.

Le présent projet de consultation prévoit d'inscrire cette base légale dans la loi sur la sécurité de l'information (LSI), adoptée par le Parlement le 18 décembre 2020. Outre l'obligation de signalement, la LSI doit aussi fixer les tâches du Centre national pour la cybersécurité (NCSC) et l'établir dans sa fonction de centrale de signalement.

L'obligation de signalement ne doit s'appliquer qu'aux cyberattaques recelant un certain potentiel de dommages. Y seront soumis les exploitants d'infrastructures critiques, c'est-à-dire de processus, de systèmes et d'installations essentiels au fonctionnement de l'économie ou au bien-être de la population. Le NCSC assumera le rôle de centrale de signalement. Il réceptionnera également les signalements de cyberincidents et de vulnérabilités des moyens informatiques transmis à titre facultatif.

Rapport explicatif

1 Contexte

1.1 Nécessité d'agir et objectifs

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[1] 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 2) 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[2]. La question d'introduire une obligation de signalement a aussi été soulevée dans le cadre des débats parlementaires concernant la révision totale de la loi 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[3], le Conseil fédéral a, le 11 décembre 2020, chargé le DFF d'élaborer jusqu'à la fin 2021 un projet de consultation prévoyant l'introduction d'une obligation de signaler les cyberattaques contre des infrastructures critiques.

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 centrale 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[4]. Le projet visant à introduire une obligation de signalement servira donc aussi à ancrer dans la loi les tâches et les compétences du NCSC.

1.2 Solutions examinées et solution retenue

1.2.1 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 volontaire fructueux nécessite une solide relation de confiance entre toutes les parties. 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

1 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

2 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

3 Cf. rapport du 25 novembre 2020 «Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen, Rechtliche Grundlagen», annexe 01 au mandat du CF du 11 décembre 2020 (disponible en allemand uniquement)

4 17.3508 Mo. Eder «Création d'un centre de compétence fédéral pour la cybersécurité»

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. Par conséquent, bien que le développement de l'échange d'informations des dernières années permette toujours le bon fonctionnement de la collaboration avec certaines entreprises et certaines organisations, il n'est plus réaliste d'envisager d'étendre ce modèle.

En cas de signalement, se concentrer sur un nombre réduit d'entreprises risque de donner une image incomplète, voire faussée de la situation. Il est en effet impossible de déterminer quel rayon d'action en Suisse possède 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 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 signalement 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 signalement apporte une plus-value aux entreprises et aux organisations.

1.2.2 Relation avec d'autres obligations de déclaration et l'échange d'informations entre autorités

L'introduction d'une obligation de signaler les cyberattaques affecte des obligations de déclaration déjà en vigueur et force à s'interroger quant à la manière et au moment où les signalements réceptionnés par le NCSC peuvent être transmis à d'autres autorités.

S'agissant de la relation avec des obligations de déclaration existantes, la possibilité d'intégrer l'obligation de signaler les cyberattaques à celles-ci a été examinée, car elle permettrait de renoncer à introduire une obligation de signalement intersectorielle. Cette option a été rejetée en raison du manque d'homogénéité des réglementations relatives aux incidents de sécurité dans les différents secteurs, voire de l'absence totale de dispositions dans certains d'entre eux. S'il existe une obligation de signaler les cyberattaques à une centrale d'enregistrement, il convient de définir quels signalements doivent être enregistrés, à quel moment et auprès de quel organe. Dans le cas d'espèce, l'obligation de signaler les cyberattaques ne remplace pas les obligations de déclaration existantes, mais les complète. Parallèlement, 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 s'applique surtout – mais pas uniquement – à l'obligation d'annonce visée à l'art. 24 de la loi révisée sur la protection des données (ci-après «nLPD»)[5], étant donné que, dans la pratique, il est fréquent que les cyberattaques entraînent des pertes de données. L'option retenue offre la possibilité à l'entreprise qui signale une cyberattaque de transmettre simultanément son annonce au NCSC et à d'autres services d'enregistrement, afin de satisfaire à d'autres obligations de déclaration. Inversement, le NCSC enregistrera aussi les signalements de cyberattaques effectués pour s'acquitter d'autres obligations de déclaration, à condition que celles-ci comprennent les éléments requis. Cette possibilité évitera aux victimes de cyberattaques de devoir signaler le même incident à différents services et selon des procédures différentes.

À cet égard, il convient également de régler les modalités de l'échange d'informations entre les autorités. Lorsque des entreprises et des organisations signalent des cyberattaques au NCSC, que ce soit à titre volontaire ou pour satisfaire à l'obligation de signalement, elles doivent être au clair sur ce qui advient de leur signalement et sur les personnes qui en prendront connaissance. Les principes de l'échange d'informations appliqués jusqu'ici doivent aussi perdurer dans cette perspective

5 Loi fédérale du 25 septembre 2020 sur la protection des données (LPD; RS **235.1**), FF *2020* 7397.

également. Toute communication de signalement, complète ou partielle, doit impérativement être approuvée par l'exploitant de l'infrastructure critique concernée ou être effectuée sous couvert d'anonymat.

La transmission d'informations permettant d'identifier les auteurs du signalement ou les entreprises concernées doit toutefois être autorisée au NCSC dans deux cas, même sans leur accord. Premièrement, une transmission aux autorités de poursuite pénale est possible si le signalement contient des informations sur une infraction grave. Le NCSC n'est certes pas soumis à l'obligation de dénoncer prévue à l'art. 22*a* de la loi du 24 mars 2000 sur le personnel de la Confédération[6], mais le responsable du NCSC peut transmettre des informations aux autorités de poursuite pénale s'il parvient à la conclusion que la gravité de l'infraction le nécessite. La transmission aux autorités de poursuite pénale n'aura pas de conséquences pénales pour l'exploitant de l'infrastructure critique, étant donné que la procédure est généralement dirigée uniquement contre les auteurs de la cyberattaque. Si, exceptionnellement, l'exploitant de l'infrastructure critique fait l'objet de poursuites pénales, l'obligation de signalement ne doit pas le conduire à s'incriminer lui-même par le biais de ce signalement. Une disposition a par conséquent été incluse pour prendre en compte le fait que personne n'est tenu de témoigner à sa propre charge, principe essentiel de la procédure pénale. Elle s'inspire de la disposition prévue pour l'obligation d'annonce en cas de violation de la sécurité des données visée dans le nouveau droit relatif à la protection des données (cf. art. 24, al. 6, nLPD).

Le deuxième cas de transmission autorisée concerne les informations pertinentes pour le Service de renseignement de la Confédération (SRC) dans le cadre de ses tâches de détection précoce et de prévention des menaces pour la sécurité intérieure ou extérieure, d'évaluation de la menace ou de service d'alerte précoce en matière de renseignement pour la protection des infrastructures critiques, conformément à l'art. 6, al. 1, let. a, al. 2 et 5, de la loi du 25 septembre 2015 sur le renseignement (LRens)[7]. Cela permet de garantir que le SRC, en sa qualité d'autorité compétente pour l'alerte précoce concernant les infrastructures critiques et pour l'évaluation de la menace, reçoit les informations nécessaires.

1.2.3 Exécution de l'obligation de signalement au moyen d'incitations et de sanctions

Parallèlement à l'introduction de l'obligation de signalement se pose la question des outils permettant de la mettre en œuvre. Trois facteurs peuvent influencer la disposition des entreprises 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 son soutien dans la gestion de l'attaque. Cette aide est proposée en guise de «premiers secours» et ne doit pas concurrencer des prestations disponibles sur le marché. Pour les exploitants d'infrastructures critiques, 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.

Le troisième facteur consiste à mettre en place des incitations négatives sous la forme d'une amende: si un exploitant d'infrastructure critique ne se soumet pas à l'obligation de signaler ou de fournir des renseignements malgré un rappel à l'ordre, le NCSC peut, en dernier recours, rendre 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. Cette possibilité de sanction relevant du droit administratif s'inspire de la loi révisée sur la protection des données, qui contient à l'art. 63 et s une disposition similaire pour le

6 RS **172.220.1**
7 RS **121**

cas d'insoumission à une décision du préposé fédéral à la protection des données et à la transparence (PFPDT).

Sur la base de sa longue collaboration avec les infrastructures critiques, le NCSC part du principe que cette disposition a plutôt un caractère symbolique et sert surtout à garantir que l'obligation de signalement 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[8] et dans l'arrêté fédéral du 21 septembre 2020 sur le programme de la législature 2019 à 2023[9]. 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, stipule 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 2023 à 2025 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[10].

La stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022 examine les modalités d'introduction d'une obligation de signaler les cyberattaques et présente la décision prise (mesure 9). Le présent projet de consultation met totalement en œuvre la mesure 9[11].

8 FF *2020* 1709, 1797
9 FF *2020* 8087, 8094
10 Budget 2022 avec PITF 2023–2025, Tome 2B, p. 11 ss, disponible à l'adresse: www.efv.admin.ch > Rapports financiers > Rapports financiers > Budget assorti d'un plan intégré des tâches et des finances
11 Cf. rapport d'août 2021 sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018–2022, p. 10, 15 s. (www.ncsc.admin.ch > Stratégie SNPC > Rapports et études)

2 Comparaison avec le droit étranger, notamment européen

Depuis l'adoption, en juillet 2016, de la directive sur la sécurité des réseaux et des systèmes d'information (directive SRI), les membres de l'Union européenne sont soumis à l'obligation de notifier les cyberincidents. Cette obligation est mise en œuvre depuis mai 2018. Elle concerne les «opérateurs de services essentiels», terme qui désigne, selon l'article 4, les entreprises privées ou des 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[12]. Le cercle des assujettis à cette obligation correspond donc dans une large mesure aux infrastructures critiques soumises à l'obligation de signalement définies dans le projet mis en consultation.

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'article 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 des mesures de sécurité à prendre, 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 (article 14).

Le projet mis en consultation se contente quant à lui de créer les bases légales nécessaires à de telles exigences dans le secteur de l'électricité. Une étude mandatée par l'Office fédéral de l'énergie (OFEN) a en effet constaté une nécessité accrue d'améliorer la cybersécurité dans ce domaine primordial pour l'approvisionnement économique et pour la sécurité du pays.[13] Dans les autres secteurs, il conviendra de déterminer par la suite si la Confédération a la compétence de fixer des normes juridiquement contraignantes en matière de cybersécurité et quelles exigences devraient, le cas échéant, être imposées dans quels domaines.

12 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 (europa.eu)

13 Stratégie de cybersécurité du 28 juin 2021 pour l'approvisionnement suisse en électricité (www.bfe.admin.ch > Approvisionnement > La numérisation du monde de l'énergie, disponible en allemand uniquement)

3 Présentation du projet

3.1 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 identifiant rapidement les méthodes d'attaque et en transmettant les alertes correspondantes.

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 signalement aux vulnérabilités des équipements informatiques. Indépendamment de 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 sur les cyberrisques (OPCy)[14]. D'une part, une telle inscription est nécessaire étant donné que le NCSC remplira la fonction de centrale d'enregistrement. D'autre part, elle permet de tenir compte de la réorganisation de l'administration fédérale dans le domaine de la cybersécurité, notamment la création du NCSC, qui n'a été entreprise que pendant les débats parlementaires sur la LSI.

3.2 Adéquation entre les tâches et les moyens financiers

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

Le NCSC utilise un formulaire électronique pour les signalements. Il est possible de l'adapter afin qu'il puisse aussi servir à la réception des signalements faisant suite à l'obligation en la matière. Les accords nécessaires avec d'autres organes qui réceptionnent également des déclarations (par ex. PFPDT, FINMA, 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 réception et la documentation des déclarations effectuées au titre de l'obligation de signalement, ainsi que leur transmission aux organes *ad hoc* aux fins d'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. Cet appui est lui aussi déjà bien rodé grâce à la longue expérience du NCSC (et de MELANI avant lui). Il faut cependant s'attendre à ce que l'introduction de l'obligation de signalement augmente la charge de travail du NCSC, d'une part, en raison de l'augmentation du nombre de déclarations et, d'autre part, parce que le NCSC sera désormais chargé d'effectuer au moins une première appréciation de l'incident et de formuler des recommandations pour sa gestion. Il convient par conséquent aussi d'augmenter l'effectif de l'équipe d'analyse technique du NCSC (GovCERT).

14 RS **120.73**

3.3 Modalités de mise en œuvre

3.3.1 Nécessité d'une base légale

Il découle du principe de légalité (art. 5, al. 1, de la Constitution, Cst.[15]) et des dispositions relatives à la législation de l'art. 164, al. 1, Cst. que l'obligation de signalement des cyberattaques doit être réglée au moins dans les grandes lignes au niveau de la loi. Le projet mis en consultation contient par conséquent les éléments essentiels de l'obligation de signaler les cyberattaques: il comporte les principaux éléments de l'obligation de signalement, notamment ses facteurs déclenchants et sa portée (cyberattaques avec potentiel de dommages), le cercle des assujettis (exploitants d'infrastructures critiques actives dans des domaines définis), le contenu des signalements et leur 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.

3.3.2 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[16]. Les actes légaux contenant déjà des dispositions relatives aux infrastructures critiques et axés sur la protection de l'ordre public (LPPCi[17], LAP[18], LMSI[19], LRens et LSI[20]) ont notamment été pris en considération pour servir de base à l'inscription dans la loi de l'obligation de signalement. 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 prévoyaient 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 également 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.

3.3.3 Dispositions d'exécution

Les prescriptions légales seront concrétisées dans une ordonnance. Celle-ci définira plus en détail les tâches du NCSC et la collaboration avec les autres services et précisera qui doit annoncer quelles cyberattaques à quel organe et selon quelle procédure. L'ordonnance intégrera les dispositions de l'actuelle OPCy qui portent sur la relation de la Confédération avec la population, et plus particulièrement avec les exploitants d'infrastructures critiques. Concernant le cercle des assujettis, il convient de vérifier dans chaque cas s'il est préférable d'apporter des précisions dans l'ordonnance relative à l'obligation de signalement ou dans les ordonnances propres au secteur dont il est question.

15 RS **101**
16 Cf. rapport du 25 novembre 2020 «Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen, Rechtliche Grundlagen», Annexe 01 au mandat du CF du 11 décembre 2020 (disponible en allemand uniquement)
17 RS **520.1**
18 RS **531**
19 RS **120**
20 Loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (LSI), FF *2020* 9665

3.3.4 Applicabilité de l'obligation de signalement

En avril 2021, le NCSC a effectué un sondage auprès des exploitants d'infrastructures critiques et des autorités au sujet du projet d'introduire une obligation de signaler les cyberattaques. Il en est ressorti qu'une telle obligation est généralement bien acceptée, à condition qu'il soit possible de la mettre en œuvre sans trop de charges administratives. L'illustration 1 montre le niveau élevé d'adhésion des personnes interrogées.

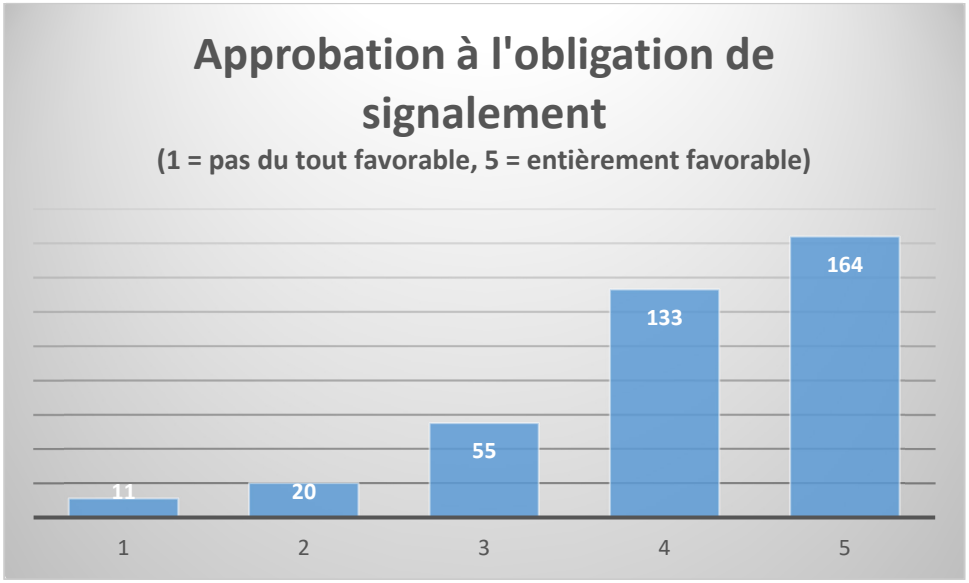

Illustration 1: Acceptation de l'obligation de signalement

Outre l'obligation d'informer le NCSC, une cyberattaque contre une infrastructure critique peut affecter d'autres processus soumis à une obligation de signalement, 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 d'annoncer les cyberattaques à la FINMA[21] est en vigueur depuis mai 2020 déjà. Ainsi, une cyberattaque devra toujours être signalée à la fois à la FINMA et au NCSC.

- 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[22].

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

La nouvelle obligation de signaler les cyberattaques ne remplacera pas les obligations de notification existantes, qui demeurent inchangées. Il est donc important que la charge soit acceptable pour les organisations tenues de signaler si elles doivent en même temps s'acquitter d'autres obligations de notification. Voilà pourquoi le NCSC mettra à disposition un système permettant la saisie électronique du signalement (formulaire, masque ou similaire). Les organisations tenues de signaler pourront décider elles-mêmes si elles souhaitent ajouter des informations au signalement électronique et l'envoyer à d'autres organes. Si d'autres services d'enregistrement devaient proposer leur aide, le masque de saisie de la déclaration pourrait aussi être conçu de telle sorte que, hormis les informations générales sur l'infrastructure, les données spécifiques qui ne concernent que l'une ou l'autre

21 Cf. art. 29 LFINMA. L'obligation générale de renseigner et d'annoncer inclut aussi les cyberincidents (cf. communication de la FINMA du 7 mai 2020 sur la surveillance)

22 Art. 24 nLPD

obligation de signalement ne soient destinées qu'au service d'enregistrement concerné. Les organisations tenues de signaler pourraient alors gérer lors de la saisie et de la transmission quelles informations sont envoyées à quel service d'enregistrement.

4 Commentaire des différents articles

Les bases légales de l'obligation de signaler les cyberattaques sont intégrées au chapitre 5 de la LSI, à l'exception de quelques adaptations mineures du chapitre 1. Le chapitre 5 a subi un remaniement de fond pour qu'il puisse aussi définir les tâches du NCSC, qui vont au-delà de l'obligation de signalement et ne sont pas spécifiquement axées sur les infrastructures critiques. Le titre du chapitre a également été adapté en conséquence («Chapitre 5: Mesures de la Confédération afin de protéger la Suisse contre les cyberrisques»).

Les principaux contenus des dispositions légales ont déjà été décrits et motivés - pour certains de manière détaillée - dans le message relatif à la LSI (FF *2017* 2872 ss) et sous les chiffres précédents. Les commentaires relatifs aux articles suivants se limitent donc à des compléments.

Chapitre 1 Dispositions générales

Dans le premier chapitre, seuls les art. 1, 2 et 5 sont modifiés. Les autres articles sont repris tels quels.

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 en complément pour fixer l'objectif en matière de cyberrisques. L'extension de la finalité de la loi permet de prendre en considération les nouveaux éléments qui accompagnent l'introduction d'une obligation de signaler les cyberattaques 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. 5 Définitions

Les définitions des let. a, b et c ne sont pas modifiées.

Let. d

La définition de «cyberincident» est reprise de l'art. 3, let. b, OPCy, avec une légère adaptation. Elle englobe également l'utilisation abusive de moyens informatiques, comme c'est le cas avec les tentatives de phishing.

Let. e

La définition de «cyberattaque» est ajoutée; il s'agit d'une forme possible de cyberincident. Il est important de distinguer «cyberattaque» et «cyberincident», car seules les attaques contre des infrastructures critiques sont soumises à l'obligation de signalement. Les cyberincidents et les vulnérabilités peuvent quant à eux être déclarés à titre facultatif par tout un chacun.

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

Aucune modification n'a été apportée aux chapitres 2, 3 et 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 divisé en trois sections.

Section 1 Dispositions générales

Art. 73a Principe

Les let. a à f décrivent les tâches du NCSC. Il s'agit d'une liste non exhaustive. En ce qui concerne la réception et le traitement des signalements (let. e), il faut préciser qu'il s'agit aussi bien des signalements volontaires de cyberincidents et de vulnérabilités que des signalements de cyberattaques contre des infrastructures critiques, lesquelles sont soumises à une obligation signalement.

Les différentes tâches ainsi que la collaboration avec les autorités en Suisse et à l'étranger font l'objet d'autres articles qui en concrétisent le contenu.

Art. 73b Traitement des signalements concernant les cyberincidents et les vulnérabilités

Depuis le 1er janvier 2020, le NCSC exploite un guichet national unique en matière de cyberrisques (cf. art. 12, al. 1, let. a, OPCy), qui enregistre et traite les signalements de cyberincidents et de vulnérabilités. La centrale d'enregistrement du NCSC a été développée à partir de MELANI, qui réceptionnait les déclarations depuis 2004. Elle est utilisée activement par les entreprises et la population: en 2020, elle a reçu 10 834 déclarations[23].

Depuis le 28 septembre 2021, le NCSC fait partie du réseau mondial gérant les vulnérabilités des systèmes informatiques et est autorisé à attribuer un numéro d'identification unique aux vulnérabilités qui lui sont signalées, conformément au système de référence international[24]. Il est donc important de préciser que le NCSC n'enregistre pas seulement les signalements de cyberincidents, mais aussi ceux de vulnérabilités.

Al. 1

Les cyberincidents et les vulnérabilités peuvent être signalés par des tiers et pas uniquement par les victimes elles-mêmes, et ce, également de manière anonyme. Le NCSC analyse les incidents et évalue leur importance pour la protection de la Suisse contre les cyberrisques. Si le signalement n'est pas anonyme, le NCSC peut, à la demande de son auteur et sur la base de ces analyses, donner son avis sur l'incident et émettre des recommandations pour la suite de la procédure. En outre, le NCSC utilise les signalements à des fins statistiques et pour avertir le public des cybermenaces. Aucune information concernant les auteurs des signalements ou les personnes concernées n'est publiée.

Le NCSC traite les déclarations en toute confidentialité. C'est une condition essentielle pour que les signalements soient faits et que la centrale d'enregistrement jouisse de la confiance des entreprises.

Al. 2

Le NCSC peut publier ou communiquer aux autorités et organisations intéressées des informations sur des cyberincidents, à condition que ces informations ne contiennent pas de données personnelles ou de données concernant des personnes morales. La publication de données personnelles dans le cas de cyberincidents est exclue. Il reste possible de publier des informations tirées du signalement avec l'accord de la personne ou de l'organisation concernées, par exemple en cas de détournement de logos lors d'attaques de phishing.

Al. 3

En revanche, en cas de vulnérabilité, la publication rapide de la faille avec indication du logiciel ou du matériel concernés peut s'avérer nécessaire pour prévenir d'autres cyberattaques. L'exploitation des vulnérabilités est l'un des modes opératoires les plus fréquents des cyberattaques. Ce n'est

23 Cf. rapport d'août 2021 sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022, p. 5 (www.ncsc.admin.ch > Stratégie SNPC > Rapports et études)

24 Cf. communiqué de presse du NCSC du 28 septembre 2021 (www.ncsc.admin.ch > Documentation > Communiqués de presse > Newslist > Le NCSC fait désormais partie du réseau mondial gérant les vulnérabilités des systèmes informatiques)

qu'avec ces informations que les utilisateurs du logiciel ou du matériel concernés peuvent prendre immédiatement les mesures nécessaires pour se protéger contre les cyberattaques. L'al. 3 constitue la base légale permettant au NCSC d'indiquer le nom du matériel et des logiciels concernés - et donc, implicitement, celui de leur fabricant - lors de la publication des vulnérabilités.

Art. 73c Transmission d'informations

L'art. 73*c* définit les conditions auxquelles le NCSC est autorisé à transmettre certaines informations contenues dans un signalement au SRC ou aux autorités de poursuite pénale (al. 1 et 2). En outre, il règle le traitement des informations au cas où une procédure pénale est engagée contre une personne ayant fait une communication (al. 3).

Al. 1

L'al. 1 stipule que le NCSC est autorisé à transmettre des informations au SRC si celles-ci sont pertinentes pour déceler à temps et prévenir des menaces contre la sécurité intérieure ou extérieure, pour évaluer le niveau de menace ou pour assurer un service d'alerte précoce dans le domaine du renseignement en vue de protéger les infrastructures critiques conformément à l'art. 6, al. 1, let. a, 2 et 5, LRens. Cette transmission est nécessaire pour que le SRC puisse remplir ses tâches également en ce qui concerne les cybermenaces. Elle se limite toutefois aux informations nécessaires à cet effet.

Al. 2

L'al. 2 règle la transmission d'informations aux autorités de poursuite pénale. L'obligation de dénoncer qui s'applique aux employés de la Confédération ne concerne pas les informations reçues par le NCSC lors du signalement d'un cyberincident ou de son analyse, car elle entre en conflit avec le principe du traitement confidentiel du signalement. Le responsable du NCSC est toutefois autorisé à transmettre des informations aux autorités de poursuite pénale. Ce faisant, il met en balance l'intérêt de l'État à une poursuite pénale et celui de la personne qui effectué le signalement à la confidentialité des informations. La possibilité de transmettre les informations après une pesée des intérêts en jeu a été prévue pour permettre au NCSC de saisir les autorités de poursuite pénale en cas d'infractions graves.

Al. 3

La disposition visée à l'al. 3 permet de garantir que la personne effectuant un signalement ne sera pas incriminée contre son gré dans le cadre d'une procédure pénale dirigée contre elle en raison des informations contenues dans la communication. En règle générale, une procédure pénale est dirigée contre les auteurs du cyberincident, c'est-à-dire contre les pirates informatiques, et non contre la personne qui a effectué le signalement. Une règle analogue à celle de l'art. 24, al. 6, nLPD a été introduite au cas où, exceptionnellement, une procédure pénale devait être dirigée contre la victime d'une cyberattaque. Cette disposition met en œuvre le principe de l'interdiction de s'auto-incriminer (*nemo tenetur*) dans le cadre de l'obligation de signaler les cyberattaques. Elle est donc particulièrement importante pour les déclarations effectuées dans le cadre de l'obligation de signaler les cyberattaques. Par ailleurs, ce privilège doit également s'appliquer aux signalements volontaires.

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. 1 et 2, le NCSC doit se faire délier du secret de fonction, conformément aux prescriptions de l'art. 320 CP, pour autant que ces informations soient des secrets pénalement protégés.

Art. 74 Soutien aux exploitants d'infrastructures critiques

En complément aux tâches générales énoncées à l'art. 73*a* et au traitement des signalements concernant les cyberincidents et les vulnérabilités visé à à l'art. 73*b*, le NCSC fournit aux exploitants

d'infrastructures critiques d'autres prestations en matière de protection contre les cyberrisques (al. 1). La définition des infrastructures critiques visée à l'art. 5 étant très large, une certaine imprécision règne quand il s'agit de déterminer si une organisation est considérée comme une infrastructure critique ou non. Pour ce faire, le NCSC s'appuie sur les secteurs et sous-secteurs mentionnés dans la stratégie nationale pour la protection des infrastructures critiques (PIC)[25].

Al. 2

À cette fin, le NCSC met des instruments à la disposition des exploitants d'infrastructures critiques. Les plus importants d'entre eux sont énumérés dans cet alinéa à titre d'exemples. Il s'agit d'une liste non exhaustive.

Let. a

L'échange d'informations est un moyen de protection essentiel contre les cyberrisques. L'important dynamisme avec lequel 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 disposition des exploitants d'infrastructures critiques une plateforme destinée à cet échange d'informations.

Let. b

Les informations sur les cyberrisques et vulnérabilités actuels et les recommandations sur les mesures de prévention se limitent aux éléments susceptibles d'être utiles aux infrastructures critiques en général. Le NCSC ne fournit pas de conseils personnalisés aux entreprises.

Let. c

Les outils techniques et les instructions de détection des cyberincidents sont en partie conçus de manière à être utiles à toutes les infrastructures critiques en général. Mais ils peuvent aussi être conçus spécifiquement pour certains groupes d'infrastructures critiques ou pour certains domaines d'activité. Ils ne remplacent pas les dispositifs de protection individuels des entreprises, mais doivent y être intégrés.

Al. 3

En cas de cyberincident, le NCSC soutient les exploitants d'infrastructures critiques en leur fournissant des conseils techniques. Le soutien technique assuré par le NCSC est fourni subsidiairement aux services informatiques disponibles sur le marché, pour autant qu'il s'agisse d'exploitants privés. C'est l'organisme responsable qui est déterminant et non la forme juridique. Par ailleurs, ce soutien n'intervient pour tous les exploitants que si le risque est imminent et que l'on est en présence d'une menace de dommages considérables.

Al. 4

En cas de cyberincident, notamment sous la forme d'une cyberattaque, le NCSC doit avoir 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 accord. L'exploitant est délié de garder le secret vis-à-vis du NCSC. La deuxième phrase constitue la base légale permettant à l'exploitant d'autoriser le NCSC à accéder à ses informations et à ses moyens informatiques sans enfreindre ses obligations légales et contractuelles de garder le secret.

Section 2 Obligation de signaler les cyberattaques contre des infrastructures critiques

25 Stratégie nationale pour la protection des infrastructures critiques 2018-2022 (www.babs.admin.ch > Autres domaines d'activités > Protection des infrastructures critiques > Stratégie nationale PIC)

Art. 74a Obligation de signalement

Cet article définit les grandes lignes de l'obligation de signalement. Il dispose que les exploitants d'infrastructures critiques sont soumis à l'obligation de signaler les cyberattaques au NCSC le plus rapidement possible après leur découverte. Il est en effet essentiel pour l'alerte précoce et la prévention que les attaques soient déclarées immédiatement après leur découverte. L'art. 74*e* précise que l'exigence d'immédiateté ne porte pas sur toutes les informations demandées, mais seulement sur le signalement initial, effectué sur la base des informations disponibles à ce moment-là.

Art. 74b Domaines

La définition des infrastructures critiques visée à l'art. 5 est très large. Elle n'est pas assez précise pour déterminer quelles sont les entreprises ou les organisations qui sont considérées comme des infrastructures critiques et, de ce fait, sont soumises à l'obligation de signalement. C'est pourquoi l'al. 74*b* dresse une liste concrète des entreprises et des organisations auxquelles s'applique cette obligation. Cette liste se fonde sur les sous-secteurs critiques définis comme tels dans la stratégie nationale pour la protection des infrastructures critiques. Pour ces domaines, le champ d'application de l'obligation de signalement est fixé, 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 manière de procéder garantit que le cercle des assujettis à l'obligation de signalement est défini avec suffisamment de clarté.

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, les hautes écoles spécialisées et les hautes écoles pédagogiques sont soumises à l'obligation de signalement.

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. L'obligation de signalement ne s'applique toutefois qu'aux tâches relevant de la puissance publique de ces autorités et de ces organisations.

Let. c: organisations chargées de tâches de droit public

Les organisations qui assument des tâches de droit public dans certains domaines sont soumises à l'obligation de signalement. La let. c énumère les activités concrètement visées par cette notion. 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 de protection et de sauvetage). Les organisations chargées de l'approvisionnement en eau potable, du traitement des eaux usées et de l'élimination des déchets sont également soumises à l'obligation de signalement.

Let. d: entreprises œuvrant dans les domaines de l'approvisionnement énergétique, 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 contre l'approvisionnement en électricité ou contre des pipelines dans d'autres États ont montré que ces infrastructures avaient été 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 soumises à l'obligation de signalement.

Let. e: banques, assurances et infrastructures de 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 importants qu'elles gèrent. Pour la fiabilité de la place financière suisse, il est important que les cyberattaques soient signalées. L'obligation de signaler les cyberattaques à l'Autorité fédérale de surveillance des marchés financiers (FINMA), qui existe déjà, est maintenue en parallèle. La FINMA et le NCSC se concerteront de manière à ce que la charge de travail pour les assujettis à l'obligation soit la plus faible possible.

Let. f: services numériques

Sont considérées comme fournisseurs de services numériques les entreprises qui proposent sur Internet des services sollicités par un grand nombre d'utilisateurs en Suisse, qui revêtent une grande importance pour l'économie numérique ou qui comprennent des services sensibles du point de vue de la sûreté et de la confiance. Il s'agit, en particulier, de fournisseurs de places de marché en ligne de taille importante, d'informatique en nuage et de moteurs de recherche. Cette énumération n'est pas exhaustive. Par «autres services numériques», on entend notamment les services dans les domaines de la gestion d'identité, des signatures ou du vote électronique. Les registraires de noms de domaine et les exploitants de centres de calcul sont également mentionnés. Des critères comme le nombre d'utilisateurs, le nombre de collaborateurs, le chiffre d'affaires ou le type d'activité seront fixés dans l'ordonnance pour concrétiser la nature des services numériques soumis à l'obligation de signalement.

Let.g: hôpitaux

Les cantons établissent des listes d'hôpitaux cantonaux et extracantonaux qui visent à assurer la couverture des besoins en soins médicaux de base sur le territoire du canton concerné. L'obligation de signaler les cyberattaques doit s'appliquer à ces hôpitaux, car il s'agit d'éviter que ce genre d'attaques ne compromettent la fourniture des soins de base.

Let. h: 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 soumises à une obligation de signalement.

Let. i: fabrication, commercialisation (ou distribution) et importation de médicaments et de dispositifs médicaux

La fabrication, la commercialisation et l'importation de médicaments revêtent une grande importance pour l'approvisionnement médical de la population. Les entreprises actives dans ces domaines sont donc soumises à l'obligation de signalement. Les fabricants et les distributeurs de dispositifs médicaux sont également soumis à cette obligation.

Let. j: assurances sociales

Les prestations des assurances sociales sont décrites en référence aux risques définis dans les dispositions générales de la loi fédérale sur la partie générale du droit des assurances sociales (LPGA[26]) afin de couvrir, si possible, toutes les branches des assurances sociales. Le législateur a renoncé à dresser une liste des différentes lois (par ex. LAI ou LAVS) pour ne pas englober uniquement les prestations légales, mais aussi les prestations surobligatoires telles que la prévoyance professionnelle ou l'assurance complémentaire à l'assurance-maladie obligatoire. En ce qui con-

26 RS **830.1**

cerne la prévoyance professionnelle, toutes les institutions de prévoyance et de libre passage, enregistrées ou non, sont concernées, mais pas la prévoyance individuelle liée ou libre (piliers 3a et 3b). Ces dernières possibilités de prévoyance sont généralement proposées par les banques et les assurances, qui sont elles-mêmes soumises à l'obligation de signalement.

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 signalement et, par exemple, limiter par des critères appropriés le cercle des destinataires des institutions de prévoyance et de libre passage soumises à l'obligation de signalement.

Let. k: 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 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[27]). Sont également considérés comme une transmission au moyen de techniques de télécommunication l'offre de capacité de transmission et les services «over the top». Ces derniers sont des transmissions d'informations via des services Internet. Parmi les exemples connus, on peut citer Skype (Microsoft), WhatsApp (Facebook), Facetime (Apple), Hangouts (Google), Signal et Threema.

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

La 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 (art. 24, al. 1, let. a, de la loi du 24 mars 2006 sur la radio et la télévision, LRTV[28]). 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. 4, let. a, LRTV). Son mandat va donc nettement plus loin que les obligations d'information des autres médias titulaires d'une concession. Des cyberattaques contre la SSR peuvent mettre en péril l'accomplissement de ces mandats.

Let. m: agences de presse d'importance nationale

Une agence de presse est considérée comme étant d'importance nationale au sens de l'art. 44*a* de l'ordonnance du 9 mars 2007 sur la radio et la télévision[29] si elle diffuse des informations portant sur les quatre régions linguistiques et qu'elle publie régulièrement des informations dans au moins trois langues nationales (cf. art. 18, let. a, de la loi du 5 octobre 2007 sur les langues[30] en relation avec l'art. 13, al. 2, de l'ordonnance du 4 juin 2010 sur les langues[31]). Concrètement, en Suisse, il ne reste que l'agence nationale de presse Keystone-ATS (cf. ordonnance COVID-19 médias électroniques[32]).

Let. n: fournisseurs de services postaux

Les entreprises qui offrent des services postaux à des clients en leur nom propre sont également soumises à l'obligation de signalement 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[33]. Le Conseil fédéral pourra exempter les petites entreprises de l'obligation de signalement au niveau de l'ordonnance. On pourrait par exemple envisager une restriction analogue à celle prévue à l'art. 4, al. 2, de la loi sur la poste pour les entreprises qui réalisent un faible chiffre d'affaires.

27 RS **784.10**
28 RS **784.40**
29 RS **784.401**
30 RS **441.1**
31 RS **441.11**
32 RS **784.402**
33 RS **783.0**

Let. o: transports publics (transport de personnes et transport ferroviaire de marchandises)

Le renvoi à la loi du 18 juin 2010 sur les organes de sécurité des entreprises de transports publics[34] permet d'englober uniquement le principal domaine des transports publics, c'est-à-dire le transport de personnes concessionnaire ainsi que le transport de marchandises et l'infrastructure de chemins de fer.

Let. p: entreprises de l'aviation civile

Cette disposition soumet à l'obligation de signaler les cyberattaques toutes les entreprises disposant d'une autorisation de l'Office fédéral de l'aviation civile.

Let. q: navigation sur le Rhin

Les ports rhénans suisses constituent l'accès de la Suisse aux mers du monde et sont d'une grande importance pour l'approvisionnement de la Suisse 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[35] et aux processus importants pour l'exploitation et le fonctionnement du port de Bâle.

Let. r: 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. L'obligation de signaler les cyberattaques ne doit s'appliquer qu'aux opérateurs qui jouent un rôle important à cet égard. Le Conseil fédéral limitera donc au niveau de l'ordonnance l'obligation de signalement dans le domaine de l'approvisionnement en biens d'usage quotidien indispensables conformément aux critères visés à l'art. 74*c*.

Let. s: fabricants de matériel et de logiciels informatiques

De plus en plus de cyberattaques d'infrastructures critiques ont lieu par le biais des fabricants de matériel et de logiciels. Les cyberpirates manipulent le matériel et les logiciels avant leur livraison aux clients finaux afin à pouvoir accéder ultérieurement aux systèmes. Les fabricants de matériel et de logiciels sont donc d'une grande importance pour la cybersécurité.

Les cyberattaques contre les fabricants de logiciels sont particulièrement importantes lorsque ceux-ci disposent d'un accès de télémaintenance. 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 et de logiciels sont soumis à l'obligation de signalement lorsque leurs produits sont utilisés dans des domaines particulièrement sensibles. Cela concerne le matériel et les logiciels de commande et de surveillance de systèmes (*industrial control systems*) (ch. 1) ainsi que l'exploitation de dispositifs médicaux et d'installations de télécommunication (ch. 2). Une attention particulière est également portée au matériel et aux logiciels utilisés pour garantir la sécurité publique (ch. 3). On pense ici, en particulier, à la communication des organisations d'intervention d'urgence ou aux systèmes d'enquête policière. En outre, les fabricants de matériel et de logiciels dotés de fonctions particulièrement sensibles (sécurité informatique, cryptage, identification, autorisation d'accès et contrôle d'accès) (ch. 4) doivent être soumis à l'obligation de signalement, car la manipulation de tels produits - qui sont justement utilisés en cas de besoin de protection accru - est dans tous les cas sensible.

34 RS **745.2**
35 RS **747.30**

Art. 74c Exceptions à l'obligation de signalement

Le cercle des assujettis visé à l'art. 74*b* est large et peut aussi englober des entreprises qui, prises individuellement, ne sont pas essentielles au bon fonctionnement de l'économie ou au bien-être de la population, bien qu'elles soient actives dans un sous-secteur critique. L'art. 74*c* précise donc que le Conseil fédéral limite davantage le cercle des assujettis. Il utilise à cette fin les critères énumérés et exempte de l'obligation de signalement les entreprises ou les catégories d'entreprises qui sont peu exposées au risque de cyberattaques, de telles attaques étant jugées improbables état donné que l'exploitation des entreprises concernées ne dépend que dans une faible mesure des moyens informatiques (let. a). L'exemption peut également advenir si la défaillance ou le dysfonctionnement n'ont qu'un faible impact sur l'économie ou le bien-être de la population, l'impact se mesurant à l'aune du nombre de personnes concernées, de la substituabilité de la prestation ou du potentiel de dommages économiques (let. b).

Art. 74d Cyberattaques à signaler

Al. 1

La portée de l'obligation de signalement, c'est-à-dire le type de cyberattaques qui doivent être signalées, doit être fixée dans la loi. L'al. 1 énumère, aux let. a à d, les critères permettant de conclure qu'une cyberattaque a un potentiel de dommages important ou une grande pertinence pour la protection d'autres infrastructures critiques. Si une cyberattaque remplit l'un de ces critères, elle doit être signalée. Les critères pourront au besoin être précisés dans l'ordonnance.

Al. 2

L'al. 2 stipule qu'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 ou certains collaborateurs de ces entreprises 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 attaques de ce genre doivent être signalées afin de pouvoir évaluer l'ampleur de la menace que les cybercriminels font peser sur les infrastructures critiques.

Art. 74e Contenu du signalement

L'al. 1 indique les informations essentielles à fournir en vue du respect de l'obligation du signalement. Le contenu concret de ces diverses informations sera précisé dans les dispositions d'exécution.

L'al. 2 précise le caractère immédiat du signalement *(«le plus rapidement possible»*) visé à l'art. 74*a*, indiquant que celui-ci ne concerne que les informations déjà connues. En cas de 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 entreprises concernées doivent par conséquent avoir la possibilité de ne transmettre les informations exigées conformément au ch. 1 que lorsqu'elles disposent de plus de détails sur la cyberattaque.

Art. 74f Communication du signalement

Al. 1

Afin que l'obligation de signalement puisse être remplie avec le moindre effort possible, il incombe au NCSC de mettre à disposition un formulaire électronique sécurisé. Compte tenu des développements technologiques, le formulaire est décrit de manière générique comme «un système sécurisé qui permet de lui communiquer le signalement». Hormis ce formulaire, il est néanmoins possible dans tous les cas de communiquer d'une autre manière (par courriel ou par téléphone) la cyberattaque au NCSC.

Al. 2

Le système de communication offre à l'auteur du signalement la possibilité de communiquer simultanément à d'autres services et autorités tout ou partie du signalement de la cyberattaque ou de ses conséquences (par ex. sur la sécurité des données ou sur le fonctionnement de l'infrastructure critique). Cette communication via le système du NCSC n'est pas soumise à obligation légale de signalement vis-à-vis d'autres services et autorités; elle est également possible pour les signalements volontaires à des organismes tiers. Il est important de noter que la communication du signalement ne peut être effectuée que par l'exploitant de l'infrastructure critique concernée. C'est lui seul qui détermine quel service ou quelle autorité - en dehors du NCSC - doit recevoir la communication de la cyberattaque ou de ses conséquences. Le NCSC ne transmet aucune communication à d'autres services ou autorités. Sont réservés les cas exceptionnels visés à l'article 73*c*, al. 1 et 2.

Al. 3

Sur demande et en collaboration avec d'autres services de communication, le NCSC peut aménager le système de manière à ce que l'exploitant d'une infrastructure critique soumis à l'obligation de signalement puisse saisir d'éventuelles données supplémentaires qui ne sont pas nécessaires pour le signalement au NCSC, afin de les transmettre à un ou plusieurs autres services de communication. Cette fonction doit servir à réduire au minimum la charge de travail des auteurs d'un signalement. Elle doit les aider, notamment en cas de cumul de plusieurs obligations de signalement, à pouvoir informer les services et autorités concernés le plus rapidement possible, en temps utile et avec le mois d'effort possible. 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.

Art. 74g Obligation de fournir des renseignements

L'obligation de fournir des renseignements est limitée aux informations dont le NCSC a besoin pour identifier le mode opératoire et la méthode d'une cyberattaque signalée (alerte précoce) et, ainsi, pour en prévenir les répercussions sur d'autres infrastructures critiques.

Art. 74h Infraction à l'obligation de signalement ou à l'obligation de fournir des renseignements

Al. 1

En cas d'infraction à l'obligation de signalement ou à l'obligation de fournir des renseignements, le NCSC doit, dans un premier temps, rendre l'exploitant de l'infrastructure critique attentif à l'infraction commise. Ce dernier a ainsi encore l'occasion de s'acquitter de ses obligations. S'il y a un malentendu à ce sujet, il est alors possible de le régler. Le NCSC est tenu de prendre ce premier contact. Il s'agit d'une condition préalable à l'adoption d'une décision en vertu de l'al. 2.

Al. 2

Dans un second temps, soit si l'exploitant ne fait rien alors même qu'il a manifestement manqué à ses obligations, le NCSC rend une décision assortie d'une menace d'amende. Dans sa décision, le NCSC doit préciser les obligations enfreintes de façon à ce qu'il n'y ait aucun doute pour l'exploitant de l'infrastructure critique sur ce qu'il doit faire ou ne pas faire. Cela facilite également le travail des autorités de poursuite pénale, qui, en cas de non-observation de cette décision, doivent établir les faits et rendre un arrêt ou une ordonnance pénale (cf. art. 74*i*).

Art. 74i Non-observation de décisions du NCSC

Cet article reprend en grande partie la réglementation prévue aux art. 63 ss nLPD en cas d'insoumission à une décision du préposé par les entreprises commerciales. Comme l'indique le message

de la loi révisée sur la protection des données[36], 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[37]). Le devoir violé qui incombe 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 (DPA)[38] 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. Cela permet d'imputer de manière appropriée la responsabilité pénale au sein des infrastructures critiques.

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 l'économie et de l'État ainsi que de bien montrer leur responsabilité 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 le niveau de cybersécurité, qui varie 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. La menace d'une amende de 100 000 francs devrait déjà amener les responsables d'infrastructures critiques à agir en conformité avec leurs obligations.

Al. 2 et 3

Pour les amendes infligées à des entreprises, la réglementation a été reprise par analogie à la loi révisée sur la protection des données (art. 64 nLPD). Jusqu'à un montant de 20 000 francs, l'amende peut ainsi être directement infligée à l'infrastructure critique à la place de la personne physique responsable, afin d'éviter une coûteuse enquête. Étant donné qu'une amende ne peut dépasser 100 000 francs, le législateur a fixé à 20 000 francs le montant pour ces cas de faible importance afin de responsabiliser les infrastructures critiques en tant que telles et de renoncer à des enquêtes supplémentaires concernant les personnes responsables. 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.

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. Le législateur a 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 sa centrale d'enregistrement, 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 de détection précoce pour les 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.

36 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, FF *2017* 6597, 6603, 6718.
37 RS **311.0**
38 RS **313.0**

Art. 75 Traitement des données personnelles

Al. 1

En lieu et place d'une description générique des services fédéraux compétents, le NCSC a été ajouté, étant précisé que celui-ci peut traiter non seulement des données personnelles, mais aussi des données sensibles et les données sensibles qui s'y rapportent. On entend par ressource d'adressage au sens de l'art. 3, let. f, LTC «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». À la let. a, le terme de «cybersécurité» a été ajouté.

Al. 2

L'al. 2 reprend l'ancien al. 3, 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 lorsque la personne concernée n'est pas informée du traitement des données ont été concrétisées.

Al. 3

Le contenu de l'al. 3 a été précisé, à savoir que la personne concernée par une utilisation abusive de ressources d'adressage doit être informée de ce fait.

Art. 76 Collaboration sur le plan national

Cet article constitue la base légale pour 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).

Des adaptations formelles ont également été apportées. On a par exemple précisé dans chaque alinéa que la collaboration est soumise à la condition qu'elle soit nécessaire à la protection des infrastructures critiques contre les cyberrisques.

Al. 1 et 2

L'échange d'informations entre le NCSC et les exploitants d'infrastructures critiques réglé à l'al. 1 ne se limite pas aux infrastructures critiques assujetties à l'obligation de signalement, mais s'adresse à toutes les infrastructures critiques intéressées ayant leur siège en Suisse.

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.

Art. 76a Assistance technique 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 détermine notamment le contenu et l'ampleur ainsi que 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 (al. 2 à 4). Un des aspects importants de la collaboration du NCSC avec ces autorités concerne l'échange d'informations sur les pirates eux-mêmes et sur leurs méthodes et tactiques.

Al. 1

Contrairement aux alinéas suivants, l'al. 1 ne règle pas l'échange mutuel d'informations, mais établit le principe selon lequel le NCSC apporte son appui au SRC dans ses tâches en procédant à des évaluations spécifiques des cyberattaques quant à leur nombre, leur type et leur ampleur ainsi qu'à des analyses techniques des cyberrisques. Ces situations 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 sa centrale d'enregistrement et l'obligation d'annonce, d'une importante source d'informations sur le niveau de menace lié aux cyberincidents. Il faut par conséquent qu'il puisse transmettre au SRC des informations sur le nombre de cyberattaques, leur type et leur ampleur. En outre, le NCSC doit pouvoir apporter son appui au SRC, en effectuant les analyses techniques des cyberattaques et en lui transmettant les 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. Un des aspects importants de la collaboration du NCSC avec ces autorités est, comme déjà mentionné, l'échange d'informations sur les agresseurs eux-mêmes et sur leurs méthodes et tactiques. 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. Aussi une base légale est-elle créée ici pour les échanges d'informations se rapportant à ces données personnelles. 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, numéro IBAN, etc.).

Les autorités habilitées en vertu des al. 2 à 4 peuvent également accéder en ligne aux informations susmentionnées. Cette procédure est indiquée en raison du grand nombre de cyberattaques et d'informations techniques associées. La transmission au SRC ou aux autorités de poursuite pénale de signalements contenant des informations sur les personnes concernées n'a lieu que dans des cas exceptionnels et reste soumise aux conditions prévues à l'art. 73*c*, al. 1 et 2.

Art. 77 Coopération internationale

Cette disposition a été adaptée sur le plan formel par une mention expresse au NCSC. En outre, le terme de «données» a été remplacé par le terme générique d'«informations», qui ne désigne pas spécifiquement les données personnelles au sens de l'art. 75. On a ajouté concrètement à propos de l'étendue, du contenu et de la finalité de l'échange d'informations que celui-ci est autorisé avec les services chargés de la cybersécurité. Le terme «cybersécurité» remplace l'expression «protection des infrastructures critiques», dont la formulation est trop restrictive, pour décrire les organisations d'envergure internationale actives dans le domaine de la cybersécurité.

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

Cet article a été supprimé au vu des modifications de bases légales relatives à la révision de la LPD. 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

Cet article n'a subi qu'une légère modification à son al. 1. On y a précisé que les données personnelles peuvent être conservées pendant cinq ans au plus à compter de leur dernière utilisation. 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 importance centrale lors des rapprochements 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. Mais comme ces données techniques renferment aussi des éléments à caractère personnel et, à ce titre, sont soumises en tant que données personnelles à la protection des données, leur durée de conservation doit être clairement délimitée. Pour des raisons tenant à la protection des données, il a été précisé dans la deuxième partie de la phrase que les données personnelles sensibles peuvent être conservées au maximum deux ans à compter de leur dernière utilisation.

Art. 80 Dispositions édictées par le Conseil fédéral

Cet article a été supprimé. Le texte de loi ayant été suffisamment concrétisé, les délégations au Conseil fédéral qui sont prévues dans cette disposition sont devenues obsolètes. La compétence d'édicter des dispositions d'exécution revient au Conseil fédéral, même sans réserve de la loi. En outre, les dispositions d'exécution prévues à la let. c (responsabilité en matière de protection et de sécurité des données) sont déjà couvertes par les art. 8, al. 3, et 33 nLPD.

Annexe 1 (Art. 89 Modification d'autres actes)

La liste des modifications d'autres actes visée à l'art. 89 de l'annexe 1 est complétée comme suit.

Loi du 23 mars 2007 sur l'approvisionnement en électricité[39]

La protection contre les cyberrisques, qui figurera désormais explicitement à l'art. 8*a* de la loi sur l'approvisionnement en électricité, contribue à la sécurité d'approvisionnement. Les mesures prévues 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 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. 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 d'approvisionnement, lors de 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 d'approvisionnement (par ex. niveau du réseau, puissance, nombre de consommateurs finaux concernés).

Le Conseil fédéral formulera dans l'ordonnance les exigences en la matière, notamment en ce qui concerne le niveau de protection visé et les audits à effectuer. Pour ce faire, il pourra s'appuyer sur les normes spécialisées 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. Des exceptions ou des allégements seront à prévoir pour les plus petits opérateurs du marché.

Étant donné le but de cette disposition, seuls entrent en ligne de compte comme autres parties en vertu de l'al. 2 les opérateurs qui exercent une influence déterminante sur la sécurité d'approvisionnement, à l'instar des grands prestataires de services du secteur de l'électricité actifs, par exemple,

39 RS **734.7**

dans le commerce et la mesure de l'énergie, la gestion de la flexibilité, le traitement des données ou la mobilité électrique.

Modification du 25 septembre 2020 de la loi sur la protection des données[40]

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 P-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, P-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 en vue de 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, révLPD, 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. À 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.

40 Loi fédérale du 25 septembre 2020 sur la protection des données (LPD), FF *2020* 7397.

5 Conséquences

5.1 Conséquences pour la Confédération

Le NCSC gère déjà à l'heure actuelle un service d'alerte qui recueille sur une base volontaire les signalements de cyberincidents. 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.

Le NCSC utilise déjà aujourd'hui un formulaire électronique pour la collecte des annonces. Il serait possible de l'adapter afin qu'il puisse aussi servir à la réception des données faisant suite à l'obligation de signalement. Un investissement initial sera certes indispensable en vue de l'harmonisation nécessaire avec les autres services collectant des annonces (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 en la matière 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.

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, de celle de MELANI). Il faut toutefois s'attendre à ce que la charge de travail du NCSC augmente en raison de l'obligation de signalement. Outre que ceux-ci seront plus nombreux, le NCSC devra 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).

Il s'agit de prendre en compte ces besoins supplémentaires dans l'actuel chantier d'extension du NCSC. Ceux-ci ne peuvent pas être suffisamment évalués indépendamment des autres tâches du NCSC, raison pour laquelle on attend le résultat de l'évaluation de l'efficacité de la cyberorganisation de la Confédération, actuellement en cours. Les besoins en ressources seront concrétisés au vu des résultats de la présente consultation dans le cadre du message.

5.2 Conséquences pour les cantons et les communes

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

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

5.3 Conséquences pour l'économie et la société

Il ne devrait y avoir aucune conséquence directe pour l'économie, la société ou l'environnement. L'économie et la société profiteront indirectement de l'introduction d'une obligation d'annoncer 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 signalement contribuera à éviter, grâce à des mesures de prévention et de défense précoce, 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 est par conséquent possible de renoncer à une analyse d'impact de la réglementation (AIR).

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

6 Aspects juridiques

6.1 Constitutionnalité

La possibilité d'introduire une obligation de signaler les cyberattaques n'est pas expressément prévue dans la Constitution fédérale. 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 protection 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 sur le plan suisse, 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 signalement 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 a en outre pour but 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, est complémentaire à la collecte d'informations supplémentaires et sert à la protection des infrastructures critiques.

En conséquence, la compétence dévolue à la Confédération de sauvegarder la sécurité intérieure et extérieure – avec des responsabilités qui, sans lui être expressément accordées, lui reviennent en tant qu'État – constitue une base constitutionnelle adéquate pour introduire des dispositions légales relatives à une obligation de signaler les cyberattaques et à un droit de signaler les cyberincidents et les points faibles.

L'art. 173, al. 2, Cst. est cité comme place réservée pour cette compétence dévolue à la Confédération en raison d'une convention formelle de technique législative[41]. Or la loi sur la sécurité de l'information mentionne en préambule (outre les art. 54, al. 1, 60, al. 1, 101, 102, al. 1, et 173, al. 1, let. a et b) également l'art. 173, al. 2, comme base de compétence déterminante. Il n'est donc pas nécessaire de compléter les dispositions constitutionnelles indiquées dans la LSI.

6.2 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.

6.3 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 signalement faite aux infrastructures critiques, elle constitue la base légale formelle du NCSC en tant que centrale d'enregistrement. 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.

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 compléter l'ordonnance en vigueur sur les cyberrisques.

41 Ch. marg. 25 des directives de la Confédération sur la technique législative (www.chf.admin.ch > Documentation > Accompagnement législatif > Directives sur la technique législative DTL)

6.4 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).

6.5 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 centrale d'enregistrement, 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 signalement constitue par conséquent une mesure conciliable avec le principe de subsidiarité (art. 5*a* en relation avec l'art. 43*a* Cst.).

Selon le principe d'équivalence fiscale statué 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 signalement, étant donné que la Confédération couvrira les coûts d'exploitation de la centrale 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 signalement n'entraînera qu'un léger surcroît de charges 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 gérées par les cantons ou les communes.

6.6 Délégation de compétences législatives

Selon le présent projet mis en consultation, 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 signalement. La loi définit les critères à appliquer à cet effet, mais il appartient au Conseil fédéral de déterminer par secteur quels critères seront appliqués et comment (par ex., en définissant des valeurs seuils appropriées).

6.7 Protection des données

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.

Le PFPDT a été consulté pour l'élaboration du projet mis en consultation. Il a également été question à cette occasion des possibilités de le coordonner avec l'obligation d'annoncer les infractions à la sécurité des données.