Berne, 13.12.2019

Obligation de déclarer les incidents graves affectant la sécurité des infrastructures critiques: solutions possibles

Rapport du Conseil fédéral
en réponse au postulat 17.3475 Graf-Litscher du 15 juin 2017

Table des matières

1 Introduction

Faut-il introduire une obligation de déclarer les incidents graves de sécurité? Les avis en Suisse sont profondément divisés sur la question. La recrudescence des cyberrisques a encore exacerbé les débats, dans un contexte très dynamique où les informations sur les pannes dues aux cyberincidents sont particulièrement précieuses.
Le présent rapport entend apporter de solides bases factuelles aux discussions concernant l'obligation de déclarer les incidents de sécurité. À cet effet, il éclaire les différentes facettes des obligations de déclarer, rappelle le contexte où s'inscrivent les obligations en vigueur en Suisse comme à l'étranger et formule plusieurs modèles de base, qui sont autant de solutions de mise en œuvre possibles.
Ce premier chapitre expose la situation initiale, revient sur les différents mandats d'examen d'une obligation de déclarer les incidents et explique la structure des chapitres suivants du rapport.

1.1 Contexte

Les sociétés modernes se caractérisent par un degré d'interconnexion élevé. De multiples interfaces relient leurs infrastructures et systèmes afin d'assurer une coordination optimale. Cet étroit maillage est à la base du bon fonctionnement de toute société. Il résulte, du moins en partie, de la numérisation des infrastructures en place. La transformation numérique simplifie et accélère les échanges entre les systèmes, au point que les frontières physiques entre eux cessent d'être pertinentes. Et comme le processus de transformation numérique n'en est qu'à ses débuts et que toutes les possibilités technologiques sont loin d'être épuisées, tout indique que l'extension des réseaux va se poursuivre.
Or en raison de cette interconnexion croissante, les perturbations ou pannes survenant dans une infrastructure spécifique risquent d'avoir des effets systémiques. Autrement dit, sachant à quel point les sociétés modernes sont tributaires du bon fonctionnement de leurs infrastructures, il vaut la peine de réfléchir à la meilleure manière d'en gérer l'interdépendance croissante.
Les échanges d'informations intersectoriels constituent un élément-clé dans la protection face aux pannes géantes guettant les infrastructures critiques[1]. Alors que les infrastructures physiques sont toujours plus interconnectées, il faut s'assurer que les services compétents s'informent mutuellement des développements en la matière, des risques et des incidents. De tels échanges permettent aux décideurs d'évaluer correctement les risques inhérents à leur infrastructure et de reconnaître à temps les dangers potentiels. L'échange d'informations joue un rôle primordial dans la protection des infrastructures critiques face aux cyberrisques. Des cyberincidents peuvent en effet toucher simultanément des organisations différentes et, en raison des interfaces entre infrastructures, constituer très vite un problème intersectoriel. Il est par conséquent important de s'avertir mutuellement de bonne heure afin de minimiser l'impact des cyberincidents.
Sans surprise, les autorités s'efforcent depuis de nombreuses années d'encourager les échanges d'informations entre exploitants d'infrastructures critiques. Beaucoup d'États ont créé à cet effet des plateformes en ligne et soutiennent activement dans ce cadre les échanges entre leurs infrastructures critiques. En Suisse, la Confédération exploite par exemple depuis 2004 une plateforme ad hoc, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI). Mais les États recourent toujours plus aussi à des instruments de réglementation, obligeant les exploitants d'infrastructures critiques à leur signaler les incidents de sécurité dont ils ont été victimes.

[1] Par infrastructures critiques on entend les processus, les systèmes et les installations qui sont essentiels pour le bon fonctionnement de l'économie ou le bien-être de la population. Il s'agit par exemple de l'approvisionnement en énergie, du transport de personnes et de biens ou encore des soins médicaux (voir la stratégie nationale pour la protection des infrastructures critiques 2018-2022).

L'entrée en vigueur en août 2016 de la directive européenne sur la sécurité des réseaux et de l'information (directive SRI) a marqué une césure importante. Cette directive établit des «exigences en matière de sécurité et de notification pour les opérateurs de services essentiels et pour les fournisseurs de service numérique», qu'il incombe aux États membres de l'Union européenne (UE) de faire respecter. Même si tous les pays n'ont encore transposé la directive SRI dans leur droit interne, elle a directement conduit beaucoup d'entre eux à introduire de nouveaux régimes de déclaration obligatoire des cyberincidents, ou à renforcer ceux en place.
En Suisse, différents travaux ont été entrepris pour déterminer s'il y a lieu d'introduire des obligations de déclarer, et comment procéder le cas échéant. Ainsi, le comité consultatif Avenir de la place financière suisse a passé en revue dans son rapport de 2017 les avantages ou inconvénients pour le secteur financier des obligations de déclarer les cyberincidents[2]. Par ailleurs, une équipe de chercheurs de l'Université de Lausanne, de l'Académie militaire et de l'Université de Saint-Gall a analysé les échanges d'informations instaurés par MELANI pour identifier les principaux obstacles ou incitations au partage de renseignements concernant les incidents de sécurité[3], tandis qu'une enquête représentative menée auprès des directeurs de petites et moyennes entreprises (PME) révélait l'absence d'avis tranché, à ce jour, parmi les PME (ni approbation ni refus) au sujet de l'introduction d'obligations de déclarer de tels incidents[4].

1.2 Mandat

Face à la tendance internationale à rendre obligatoire la déclaration des incidents de sécurité et comme la discussion à ce sujet n'est pas aussi avancée en Suisse, il s'agit aujourd'hui d'élaborer des bases qui permettent de savoir s'il y a lieu d'introduire des obligations de déclarer, et le cas échéant lesquelles. Le Conseil fédéral, le Parlement et le groupe d'experts Avenir du traitement et de la sécurité des données ont par conséquent formulé une série de mandats d'examen:

- **Postulat 17.3475 Graf-Litscher «Infrastructures critiques. Prévoir une obligation de signaler les incidents graves de sécurité»:** Le Conseil fédéral est chargé d'établir un rapport sur les possibilités qui s'offriraient, d'une part, de soumettre, critères à l'appui, les exploitants d'infrastructures critiques à une obligation générale de signaler les incidents de sécurité et autres défaillances potentiellement graves, d'autre part, de systématiser l'analyse des informations reçues et constatations effectuées, enfin, de mettre sur pied un système d'alerte rapide, de conseil et de défense.

- **Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), mesure 9 «Examen d'une obligation de notifier les cyberincidents et décision quant à son introduction»:** Afin d'améliorer le tableau de la situation, il convient d'étudier l'introduction d'une obligation de notifier les cyberincidents, et de statuer sur sa mise en place. Plusieurs questions seront examinées au préalable: à qui s'appliquerait une telle obligation, quels seraient les incidents concernés, à qui devrait-on les signaler, et une obligation de notifier permettrait-elle d'améliorer notablement l'état des lieux? Différentes solutions possibles seront élaborées pour la mise en œuvre de l'obligation de notifier dans les différents secteurs, en montrant les bases légales à prévoir. Ce travail sera accompli avec la participation des autorités compétentes, du secteur privé et des associations de branche, en coordination avec la stratégie nationale pour la protection des infrastructures critiques et en tenant compte des développements internationaux. La décision d'introduire une obligation de

[2] Comité consultatif Avenir de la place financière suisse, Rahmenbedingungen für die Versicherbarkeit und ein effizientes Management von Cyber Security Risiken.
[3] Mermoud et al., To share or not to share: a behavioral perspective on human participation in security information sharing, Journal of Cybersecurity, 2019, vol. 5, n° 1.
[4] gfs-zürich, Cyberrisiken in Schweizer KMUs, 2017.

notifier les cyberincidents se prendra sur la base de ces vérifications et, le cas échéant, les démarches nécessaires seront entreprises.

- **Stratégie nationale pour la protection des infrastructures critiques, mesure 8:** Examiner la possibilité d'élaborer un projet de base visant à inscrire dans la loi l'obligation pour les exploitants d'infrastructures critiques d'informer les autorités compétentes en cas de défaillance ou de problème de sécurité important.

- **Rapport du groupe d'experts concernant le traitement et la sécurité des données, recommandation 28 «Obligations de notifier»:** La Confédération soumet les exploitants d'infrastructures critiques à une obligation de notifier les cyberincidents. Elle élabore la base légale nécessaire à cet effet en collaboration avec les autorités compétentes, le secteur privé et les associations concernées, compte tenu également des développements internationaux en la matière.

Le présent rapport fait la synthèse des travaux entrepris à ce jour dans le cadre de ces mandats. Il s'appuie essentiellement sur les résultats d'une étude externe commandée, qui dresse un état des lieux des obligations de déclarer en vigueur en Suisse, analyse les solutions adoptées à l'étranger et comporte encore des entretiens avec des experts suisses[5]. À partir des connaissances ainsi acquises, des modèles de base ont été créés, qu'il s'agira d'affiner et de développer encore dans une discussion à venir. L'étude se concentre sur les obligations de déclarer les cyberincidents, non que les experts estiment urgent d'agir sur ce plan, mais parce que les obligations de déclarer introduites dans d'autres pays se réfèrent explicitement aux cyberincidents. Il reste à savoir si et comment, de façon générale, les modèles proposés pourraient être utilisés pour déclarer les incidents de sécurité, et comment les modèles de déclaration obligatoire des cyberincidents pourraient être conciliés avec les obligations de déclarer déjà en vigueur pour d'autres incidents de sécurité.

1.3 Structure du rapport

Le rapport décrit au chapitre suivant (chapitre 2) les questions que soulèvent, le cas échéant, l'introduction d'obligations de déclarer ou l'extension des obligations existantes. Il convient de souligner qu'au-delà de la question fondamentale de l'opportunité d'introduire de nouvelles obligations de déclarer, il s'agit encore de préciser la finalité des obligations de déclarer, leurs destinataires et leur teneur, ainsi que leurs modalités éventuelles.
Les chapitres 3 et 4 exposent la situation actuelle. Ils signalent les obligations de déclarer en vigueur en Suisse et décrivent celles ayant été introduites au cours des dernières années à l'étranger. Ce panorama montre où la Suisse se situe aujourd'hui par rapport à d'autres pays, et quelles solutions ont été choisies dans d'autres États ayant introduit des obligations de déclarer.
À partir des comparaisons internationales établies, de l'inventaire des obligations de déclarer en Suisse ainsi que des entretiens menés avec des experts, le chapitre 5 présente pour l'obligation de déclarer quatre modèles de base conçus dans l'étude consacrée à la question (*Prüfung einer Meldepflicht bei Sicherheitsvorfällen*). Le rapport s'achève (chapitre 6) par un bref aperçu de la procédure à suivre pour déterminer s'il y a lieu d'introduire des obligations de déclarer en Suisse, et le cas échéant comment.

[5] PwC Schweiz, Prüfung einer Meldepflicht bei Sicherheitsvorfällen, octobre 2019.

2 Questions pertinentes pour l'introduction d'obligations de déclarer

La discussion sur les obligations de déclarer tend à se réduire à une question de principe, à savoir si leur introduction fait sens ou non. Or pour en juger, il faut d'abord préciser à quel genre d'obligations de déclarer on pense, qui serait le destinataire des déclarations et à quelles conséquences les assujettis devraient concrètement s'attendre en cas d'instauration d'un tel régime. Les entretiens menés à l'occasion d'une récente étude (*Prüfung einer Meldepflicht bei Sicherheitsvorfällen*) ainsi que l'analyse des obligations de déclarer existant dans d'autres pays ont fait ressortir l'importance de soigneusement traiter toutes ces questions lors de la conception de modèles d'obligation de déclarer. Le présent chapitre commence donc par décrire les principales questions à clarifier au cours de l'élaboration et de l'évaluation des solutions possibles en matière d'obligation de déclarer.

2.1 Finalité des obligations de déclarer

Les obligations de déclarer ont pour but d'assurer une protection accrue de l'économie ainsi que de l'État. Mais si l'on entre dans les détails, les arguments en faveur de l'introduction d'obligations de déclarer diffèrent de manière significative. Cinq grandes raisons peuvent amener les autorités à soumettre les incidents de sécurité à une obligation de déclarer:

- **Obligation de surveillance de l'économie incombant à l'État:** le législateur ordonne à l'État de désigner des régulateurs (dont le rôle diffère d'un secteur à l'autre) pour surveiller des secteurs économiques spécifiques. Or les autorités exerçant cette fonction doivent être au courant des perturbations existantes afin d'adopter, en cas de besoin, des mesures propres à garantir le bon fonctionnement du secteur concerné.
- **Prévention des incidents de sécurité:** l'introduction d'obligations de déclarer contraint les entreprises à s'intéresser aux incidents de sécurité. Elles doivent se doter d'une structure de processus qui leur permette d'identifier et de déclarer à temps les incidents. L'obligation de déclarer a ainsi pour effet de renforcer la prévention globale des incidents de sécurité.
- **Évaluation de la menace:** les autorités ont toujours plus besoin d'informations fournies par les milieux économiques afin de juger de l'état actuel des menaces. Par exemple, il se peut que des cyberattaques prennent pour cibles des entreprises précises et que l'État ne s'en aperçoive pas, ou alors trop tard, sans déclaration de leur part.
- **Alerte rapide grâce aux échanges d'informations:** dans un monde d'interconnexion et donc d'interdépendance croissante, les échanges concernant les incidents affectant la sécurité sont devenus prioritaires. En introduisant des obligations de déclarer, les autorités peuvent être sûres que toutes les organisations essentielles au bon fonctionnement de l'État et de l'économie disposent rapidement de précieuses informations portant, par exemple, sur les failles de sécurité découvertes ou sur de nouveaux vecteurs d'attaque.
- **Réaction coordonnée:** seule la déclaration des incidents rend possible une réaction coordonnée. Du fait des interdépendances mutuelles, il est crucial pour maîtriser un incident que le service appelé à prendre des décisions importantes dispose au plus vite de toutes les informations pertinentes, avec un maximum de détails.

Ces divers objectifs ne s'excluent pas nécessairement. Mais il est important, au stade de la conception des obligations de déclarer, d'en définir clairement le but principal. S'il s'agit par exemple du devoir de surveillance de l'État, elles seront définies à l'égard des autorités de régulation, alors que les modèles prévoyant une centrale d'enregistrement conviennent mieux dans une optique d'évaluation de la menace, de détection précoce des risques ou de réaction coordonnée. Le but visé s'avère également déterminant pour le déroulement de la déclaration. S'il s'agit de la détection

précoce ainsi que de la coordination en cas d'incident, la déclaration devra par exemple être faite au plus vite, alors que le facteur temps importe moins quand on évalue la menace. D'où la nécessité de définir clairement, lors de toute discussion sur l'introduction d'obligation de déclarer, quel en est l'objectif principal et quels sont les autres effets attendus.

2.2 Étendue des obligations de déclarer

L'étendue des obligations de déclarer constitue également une question centrale à tirer au clair pour juger de la nécessité éventuelle d'introduire un tel régime. Elle concerne aussi bien le groupe cible de l'obligation de déclarer (qui doit déclarer) que son contenu (ce qu'il faut déclarer). En ce qui concerne le cercle des destinataires, la pratique qui s'est imposée dans de nombreux pays limite le champ d'application aux exploitants d'infrastructures critiques. La formulation de la directive SRI, qui exige de prévoir de telles obligations «pour les opérateurs de services essentiels et pour les fournisseurs de service numérique», tout en laissant les États membres libres de déterminer quels services entrent dans cette définition, montre toutefois à quel point les avis divergent sur la question.
Il est encore plus épineux de déterminer quels événements concrets sont assimilables à des incidents de sécurité et à partir de quand un incident doit être déclaré. Tandis que certains modèles définissent ici des valeurs seuils, d'autres renoncent délibérément à le faire, avec pour résultat une plus grande flexibilité pour aménager l'obligation de déclarer, mais aussi un plus grand flou. La question des incidents à déclarer relève du casse-tête, notamment dans le cas des cyberincidents. Alors que les cyberrisques évoluent très rapidement, il est difficile d'estimer parmi les innombrables incidents à déplorer quelles sont les informations à collecter en priorité.

2.3 Définition des points de contact et de leurs tâches

En plus de définir qui doit déclarer quoi, il faut encore préciser à qui sera faite la déclaration. Comme indiqué plus haut il peut être plus judicieux, selon la finalité de l'obligation, d'établir le point de contact au niveau des secteurs d'activité, ou alors d'instituer un guichet unique au niveau national. Il existe une certaine marge de manœuvre sur la question, avec diverses formes mixtes entre points de contact centralisés et points de contact décentralisés.
Il est toutefois nécessaire de clarifier quels sont les services les plus adéquats comme points de contact, cette question étant directement liée à celle de la finalité de l'obligation de déclarer. Si des entreprises sont tenues de signaler les incidents survenus aux autorités, ces dernières ont quant à elles le devoir de traiter les informations fournies afin qu'il en résulte une plus-value pour toute la société. Il faut ici déterminer les tâches que le point de contact assume et l'usage qu'il fera des informations reçues, avec qui il les partage et sous quelle forme.
En outre, le surcroît d'effort exigé des déclarants dépend du type de points de contact créés. Il est donc important, pour que les obligations de déclarer soient bien acceptées, de limiter autant que possible la charge bureaucratique. Il s'agit surtout d'éviter que les victimes ne doivent signaler un même incident à plusieurs services.

2.4 Organisation des processus

Outre la question de la finalité des obligations de déclarer et celle des points de contact adéquats, il s'agit de définir les prescriptions applicables au processus de déclaration. Concrètement, il faut déterminer dans quel laps de temps la déclaration doit être faite, si elle peut être anonyme (et le cas échéant quel dispositif permettrait de s'assurer du respect de l'obligation de déclarer), et quelles sont les sanctions à prévoir si l'obligation n'est pas respectée.
Tous ces éléments qui, à nouveau, dépendent directement de l'objectif visé, influencent dans une large mesure l'acceptabilité des obligations de déclarer. Or les entretiens menés avec des représentants des secteurs critiques pour l'étude *Prüfung einer Meldepflicht bei Sicherheitsvorfällen* ont clairement montré l'importance d'associer les parties prenantes à l'organisation des processus, afin de trouver une solution viable pour tout le monde.

3 Obligations de déclarer en vigueur en Suisse

Avant de formuler pour la Suisse tout nouveau modèle d'obligation de déclarer en cas d'incident, il est important de connaître ce qui existe déjà. En l'occurrence, une analyse des bases juridiques en vigueur a montré que les secteurs critiques sont déjà assujettis à diverses obligations de déclarer les incidents affectant leur sécurité.
Les auteurs de l'étude *Prüfung einer Meldepflicht bei Sicherheitsvorfällen* ont identifié pour les neuf secteurs critiques de la Suisse (énergie, élimination des déchets, finances, santé, information et communication, alimentation, sécurité publique, transports et autorités) les obligations de déclarer imposées aux exploitants dans la législation sectorielle. Ces bases légales figurent dans ladite étude, et le présent chapitre s'en tient à résumer brièvement les conclusions les plus pertinentes pour la question de l'introduction d'une obligation générale de déclarer.

3.1 Bases et portée des obligations de déclarer existantes

Les obligations de déclarer varient d'un secteur à l'autre. Dans les marchés fortement régulés, à l'instar de l'énergie nucléaire, elles sont formulées de manière différenciée et des sanctions sont définies. Des règles très détaillées existent également dans l'aviation civile, secteur fortement réglementé au niveau international. Dans d'autres secteurs, les obligations de déclarer se limitent aux «événements extraordinaires» (art. 8, al. 3, LApEl), à «tout fait important susceptible de l'intéresser» (art. 29, al. 2, LFINMA) ou à «toute perturbation de l'exploitation de leurs réseaux touchant un nombre élevé de clients» (art. 96, al. 1, OST). En général, de telles dispositions ne prévoient ni un seuil à partir duquel une déclaration devient obligatoire, ni des sanctions en cas de manquement.
Faute de normes différenciées dans la plupart des secteurs, on n'y trouve pas non plus d'obligation de signaler les cyberincidents. Les obligations de déclarer formulées en termes généraux incluent les cyberincidents à partir du moment où ils causent de graves perturbations. Les attaques déjouées ou les incidents sans conséquences graves se prêteraient bien à un échange actif d'informations, mais les déclarations en la matière se font sur une base volontaire, tantôt à la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) de la Confédération, tantôt à des Computer Emergency Response Teams (CERT) sectoriels. Les exploitants d'infrastructures critiques n'ont toutefois aucune obligation légale de participer à cet échange d'informations.
Outre l'obligation de déclarer les incidents de sécurité, de nombreuses lois astreignent les entreprises à informer le régulateur. Les sociétés assujetties sont ainsi tenues de satisfaire aux demandes de celui-ci. En vertu de ces obligations de renseigner, les régulateurs sont en mesure de recueillir des informations même sur des incidents n'ayant pas eu de lourdes conséquences.

De façon générale, il ressort de l'examen des bases juridiques et de l'étendue des obligations de déclarer existantes que dans de nombreux secteurs (mais pas dans tous les sous-secteurs), l'exigence d'une obligation de déclarer les incidents graves affectant la sécurité est en principe déjà remplie. Mais les obligations sont habituellement formulées en termes très généraux, elles ne sont d'ordinaire pas assorties de sanctions et se limitent à une simple déclaration faite au point de contact du secteur concerné.

3.2 Points de contact existants

Les obligations de déclarer figurent dans différentes bases légales sectorielles, qui désignent des points de contact différents. Il s'agit typiquement des autorités de régulation et de surveillance des sous-secteurs. Dans certains cas, à l'instar des sous-secteurs «Alimentation» et «Élimination», les points de contact sont définis non pas à l'échelon national, mais à l'échelon cantonal. Depuis 2004, les cyberincidents peuvent être déclarés à un guichet unique, soit la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI). Divers secteurs (p. ex. finances, recherche, énergie) possèdent en outre leur propre point de contact pour le signalement de ces incidents (CERT sectoriel). Dans le cas de MELANI comme des CERT sectoriels, les déclarations ont toutefois un caractère facultatif.
Le principe de la compétence des autorités de régulation facilite aux entreprises la déclaration des incidents, car celles-ci savent d'ordinaire à qui s'adresser du fait de leurs échanges réguliers avec leurs autorités compétentes. Inversement, les autorités de régulation sont à même de juger, grâce à leurs connaissances spécialisées, de l'importance que revêt un incident pour leur secteur, et si nécessaire d'adopter les mesures utiles.
Les entretiens menés avec des experts issus des milieux économiques pour l'étude *Prüfung einer Meldepflicht bei Sicherheitsvorfällen* ont cependant révélé un réel scepticisme, en cas d'extension de l'obligation de déclarer en vigueur au-delà des incidents particulièrement graves, à l'égard de tout modèle prévoyant des déclarations à l'autorité de régulation. À plus forte raison dans le contexte des cyberincidents. Premièrement, si les déclarations parviennent à l'autorité de régulation, les informations ne circuleront pas entre les secteurs, ce qui est pourtant crucial lors de cyberincidents. Deuxièmement, les déclarations à l'autorité de régulation sont problématiques dans l'optique des entreprises, qui s'exposent ainsi à des examens complémentaires. Cette situation peut les amener à ne rien dire, à faire des déclarations incomplètes ou alors seulement après des clarifications juridiques approfondies, ce qui aurait de graves inconvénients en cas de cyberincident. Troisièmement, si les autorités de régulation possèdent les connaissances sectorielles nécessaires, elles ne sont généralement pas expertes en matière de cybersécurité.
Autrement dit, les points de contact qui existent aujourd'hui sont conçus en fonction des obligations de déclarer figurant dans la législation. Ils sont aptes à enregistrer les graves incidents de sécurité. En cas d'extension des obligations de déclarer – notamment aux cyberincidents –, il s'agira d'examiner si et comment on devrait adapter le système actuel, avec ses nombreux points de contact en place dans de multiples secteurs.

4 Obligations de déclarer en vigueur à l'étranger

Dans les pays comparables à la Suisse, les obligations de déclarer ne constituent pas non plus une nouveauté pour les entreprises, et existent même depuis longtemps dans de nombreux secteurs. En réponse à l'interconnexion numérique et à l'exposition croissante aux cyberrisques, les obligations de déclarer ont parfois été sensiblement étendues et renforcées au cours des dernières années.
L'impulsion est surtout venue des décisions de l'UE ayant abouti à l'introduction en 2016 de la directive européenne sur la sécurité des réseaux et de l'information (directive SRI). Depuis lors, il est bien clair que tous les États membres de l'UE sont tenus d'introduire des obligations de déclarer pour les opérateurs de services essentiels et les fournisseurs de service numérique.
Les solutions choisies par d'autres pays offrent un intéressant matériel de référence pour la décision à prendre sur l'introduction d'obligations de déclarer en Suisse, avec leurs modalités éventuelles.
L'étude *Prüfung einer Meldepflicht bei Sicherheitsvorfällen* a analysé les obligations de déclarer en vigueur en Allemagne, en Autriche, en France, en Norvège et en Israël (les résultats détaillés de cette analyse y sont présentés). On peut en tirer les enseignements suivants pour les questions de principe décrites au chapitre 2:

- **Finalité des obligations de déclarer:** les obligations de déclarer introduites ces dernières années (qui concernent surtout les cyberincidents) ont en général pour but principal la détection précoce par le biais d'échanges d'informations. La directive SRI, qui a conduit de nombreux États membres de l'UE à introduire des obligations de déclarer, poursuit expressément un tel objectif.
  Cet aspect est également prioritaire, avec la coordination en cas d'incident, dans d'autres pays comme Israël et la Norvège. Les obligations de déclarer sont conçues comme un devoir de coopération et d'assistance mutuelle dans le cadre de l'échange d'informations. À cet égard, les récentes obligations de déclarer diffèrent des obligations traditionnelles ayant pour but premier de renforcer la fonction de surveillance des régulateurs d'un secteur.

- **Étendue des obligations de déclarer:** tous les États examinés se concentrent, au niveau des destinataires, sur les infrastructures critiques. La directive SRI a élargi le groupe cible aux «fournisseurs de service numérique». Soit par exemple en Allemagne les fournisseurs de moteurs de recherche en ligne, les services d'informatique en nuage ou les marchés en ligne[6]. Dans l'ensemble, beaucoup de pays semblent avoir du mal à délimiter précisément les destinataires des obligations de déclarer.
  Dans tous les pays examinés, il faut déclarer en priorité les incidents graves. Les valeurs seuils sont toujours fixées par secteur, d'où des différences dans le traitement des cyberincidents. En Allemagne et en Autriche, ceux-ci ne sont pas répertoriés séparément et figurent parmi les obligations de déclarer prévues dans les sous-secteurs. En France comme en Israël, les cyberincidents sont répertoriés séparément. La Norvège, enfin, est en train de légiférer dans ce domaine.

- **Points de contact:** aucun des pays examinés n'a désigné de guichet unique pour les déclarations concernant la sécurité. Les incidents doivent être signalés à l'autorité compétente dans le secteur concerné. La plupart des États ont toutefois opté pour des solutions plus centralisées dans le cas des cyberincidents. Tantôt ils doivent être directement déclarés à une agence étatique (p. ex. en Allemagne le Bundesamt für Sicherheit in der Informationstechnik BSI, ou en France l'Agence nationale de la sécurité des systèmes d'information ANSSI), tantôt ils parviennent à un service central par le biais des CERT sectoriels.

[6] https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/DigitaleDienste/digitaledienste_node.html

- **Organisation des processus:** l'aménagement des obligations de déclarer diffère d'un pays à l'autre, et même entre les secteurs d'activité d'un même pays. Ainsi, aucun pays ne fixe partout les mêmes délais, qui sont définis par secteur.
  À propos des sanctions, le Règlement européen sur la protection des données joue un rôle important pour les États membres de l'UE, en prévoyant des amendes relativement élevées pour les incidents de protection des données n'ayant pas été déclarés. L'Allemagne, l'Autriche et la France ont expressément défini des sanctions en cas de non-déclaration d'incidents affectant la sécurité des infrastructures critiques. Par contre, ni la Norvège ni Israël n'ont défini de sanctions dans leur ordre juridique pour de tels cas.
  Tous les pays n'autorisent pas les déclarations anonymisées pour les infrastructures critiques. C'est absolument exclu en France et en Autriche, tandis qu'en Allemagne les déclarations anonymes ne sont admises que si les incidents n'ont pas eu de suites graves. En Norvège, il est en principe possible de faire une déclaration anonyme, sauf dans le secteur financier. Israël par contre accepte les déclarations anonymes.

En ce qui concerne la mise en œuvre des obligations de déclarer, les comparaisons internationales font ressortir l'importance d'harmoniser les systèmes en place basés sur des déclarations faites aux régulateurs avec les nouvelles obligations prévues pour les cyberincidents. Ce n'est pas simple, car les réglementations existantes ont un caractère sectoriel marqué, alors que pour les cyberincidents il faudrait autant que possible introduire des règles intersectorielles, de façon à renforcer efficacement la détection précoce. Les diverses solutions adoptées dans les pays examinés confirment toutefois qu'il serait parfaitement possible d'adapter les obligations de déclarer aux besoins existants ainsi qu'aux structures en place.

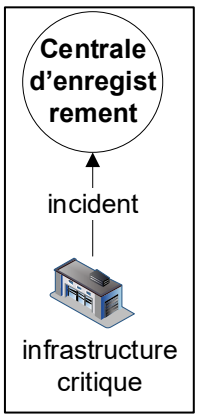
5 Solutions possibles pour les obligations de déclarer en Suisse

À partir de leur propre analyse des obligations de déclarer en vigueur en Suisse, d'entretiens menés avec des experts issus des milieux économiques et du secteur public, et aussi de divers exemples internationaux, les auteurs de l'étude *Prüfung einer Meldepflicht bei Sicherheitsvorfällen* ont identifié quatre solutions possibles pour d'éventuelles obligations de déclarer en Suisse:

1. **Introduction d'une centrale d'enregistrement des incidents affectant la sécurité**
2. **Extension et renforcement des points de contact dans les secteurs**
3. **Points de contact décentralisés et centrale d'enregistrement des cyberincidents**
4. **Absence d'obligation de déclarer**

Ce chapitre décrit brièvement les quatre modèles de base de l'étude, en faisant à chaque fois ressortir leurs conséquences pour les questions de base décrites au chapitre 2 (finalité de l'obligation de déclarer, étendue, points de contact, organisation des processus).

5.1 Centrale d’enregistrement

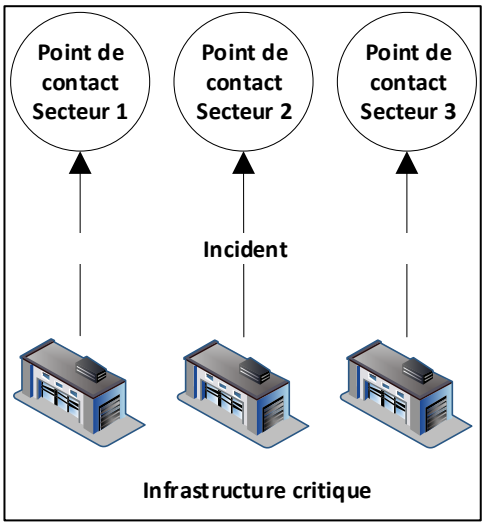


Description: une centrale d’enregistrement intersectorielle est mise sur pied pour tous les incidents affectant la sécurité des infrastructures critiques.
Avantages: toutes les informations sont enregistrées de manière centralisée, ce qui facilite la coordination intersectorielle. Chacun sait à qui doivent parvenir les déclarations, et les processus sont identiques pour tous les secteurs.
Inconvénients: une centralisation poussée exigerait de modifier en profondeur le système actuel et soulèverait d’épineuses questions de compétence dans les relations entre la centrale d’enregistrement et les régulateurs. En outre, une centrale ne pourrait pas (ou alors difficilement) tenir compte des spécificités de chaque secteur dans l’aménagement de l’obligation de déclarer.

Appréciation du modèle en fonction des questions de base:

- **Forces et faiblesses par rapport à la finalité des obligations de déclarer:** une solution centralisée présente des avantages dans l’optique d’un état des lieux des menaces, pour la détection précoce comme pour la coordination des réactions, étant donné que toutes les informations convergent au même endroit. Un tel modèle ne convient toutefois guère au renforcement de l’obligation de surveillance des régulateurs, qui ne recevraient plus les informations ou alors seulement de manière indirecte, par le biais de la centrale d’enregistrement. Autrement dit, le renforcement de la prévention dans les entreprises ne se poursuivrait pas au rythme actuel.
- **Étendue des obligations de déclarer:** il faudrait définir de manière large le groupe cible en raison de la difficulté de procéder, avec une solution centralisée, à une sélection différenciée des entreprises assujetties. En outre, il serait très délicat de définir avec un tel modèle des valeurs seuils pour l’obligation de déclarer, sachant que les valeurs judicieuses diffèrent d’un secteur à l’autre. Or des solutions adaptées aux besoins sectoriels ne sont guère réalisables dans un modèle centralisé.
- **Effets sur les points de contact existants:** le modèle bouleverserait le système actuel et sa mise en place impliquerait un lourd effort. Il faudrait revoir diverses compétences juridiques et définir la relation entre la centrale d’enregistrement et les régulateurs compétents au niveau sectoriel.
- **Organisation des processus:** il serait difficile de mettre en place des échéances judicieuses dans un tel modèle, étant donné que l’urgence d’une déclaration n’est pas la même dans tous les secteurs. En revanche, des procédures de déclaration anonymes seraient possibles. Par ailleurs, le problème des compétences juridiques se reposerait pour les sanctions en cas de non-déclaration, car la centrale d’enregistrement et le régulateur sectoriel constitueraient deux entités.

5.2 Points de contact décentralisés

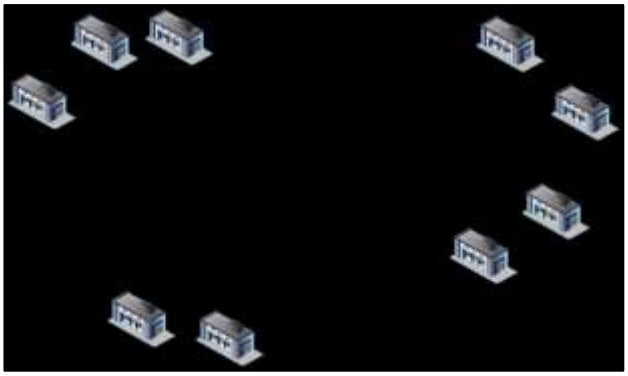


Description: les points de contact décentralisés dans les différents secteurs sont renforcés et les obligations de déclarer étendues (notamment en cas de cyberincident). Des points de contact sont mis en place dans les secteurs qui en étaient dépourvus.
Avantages: la mise en œuvre du modèle serait plutôt rapide, car il étend les structures existantes. Les bases juridiques requises pour les obligations de déclarer existent déjà dans différents secteurs. Et comme les régulateurs connaissent bien leur secteur, ils pourraient adapter l'obligation de déclarer à leurs besoins concrets.
Inconvénients: la coordination transversale n'est pas garantie. Les points de contact existants ne sont pas conçus pour recueillir les déclarations de cyberincidents.

Appréciation du modèle en fonction des questions de base:

- **Forces et faiblesses par rapport à la finalité des obligations de déclarer:** une extension décentralisée des obligations de déclarer renforcerait le rôle des régulateurs. Les objectifs intersectoriels (p. ex. améliorer la détection précoce, coordonner la réaction, dresser un état des lieux des menaces) ne seraient atteignables que si un fructueux échange d'informations avait lieu entre les régulateurs sectoriels. Or il s'agit d'un réel défi dans le cas des cyberincidents.
- **Étendue des obligations de déclarer:** les secteurs décident eux-mêmes quelles entreprises sont assujetties et quels incidents devront leur être signalés. L'étendue des obligations de déclarer peut ainsi être fixée de façon optimale.
- **Effets sur les points de contact existants:** le système actuel est étendu. Là où c'est nécessaire, les bases juridiques en vigueur concernant les points de contact seront complétées. Il faudrait examiner comment intégrer MELANI au système, en tant que point de contact des cyberincidents. De même, il faudrait trouver un moyen de vaincre les réticences des entreprises à toute extension de leurs obligations de déclarer les incidents aux points de contact des régulateurs.
- **Organisation des processus:** chaque régulateur fixe séparément, dans son secteur, les délais à respecter pour les déclarations obligatoires. Il définit aussi d'éventuelles sanctions. La possibilité de faire des déclarations anonymes serait limitée dans la plupart des secteurs car dans la pratique, le régulateur serait en mesure de découvrir rapidement quelle entreprise lui a transmis une telle déclaration.

5.3 Points de contact décentralisés et centrale d'enregistrement des cyberincidents



Description:
Ce modèle prévoit une forme mixte pour les points de contact. Le premier interlocuteur en cas d'incident de sécurité est le point de contact défini au niveau du secteur. Une centrale d'enregistrement analyse l'ensemble des cyberincidents. Il faudra encore déterminer si les déclarations doivent être directement adressées à cette centrale ou alors transiter par un point de contact sectoriel (CERT sectoriel).

Avantages: le modèle combine les solutions en place dans les secteurs avec une centrale d'enregistrement des cyberincidents. Les incidents de sécurité physique, qui intéressent d'abord le secteur et le régulateur, restent dans le secteur, tandis que les informations sur les cyberincidents sont diffusées à plus grande échelle. Le modèle offre une grande flexibilité d'aménagement.
Inconvénients: il reste un grand nombre de points de contact différents. Les tâches et les canaux de communication entre ces services devront être soigneusement définis. Comme plusieurs points de contact sont en place, les entreprises ne savent pas forcément à qui s'adresser, notamment parce qu'il n'est pas toujours aisé de distinguer entre les incidents physiques et les cyberincidents.

Appréciation du modèle en fonction des questions de base:

- **Forces et faiblesses par rapport à la finalité des obligations de déclarer:** le modèle reste ancré au niveau des secteurs, et donc la surveillance incombe toujours aux régulateurs. Il devient ainsi possible d'instaurer dans le cyberespace des systèmes de détection précoce intersectoriels, de renforcer la coordination en cas d'incident et de représenter de façon complète la situation de la menace. Il sera toutefois important de définir clairement les tâches et les canaux de communication entre les points de contact, ainsi que de préciser aux exploitants d'infrastructures critiques quels sont les incidents à déclarer et à qui la déclaration doit être faite.
- **Étendue des obligations de déclarer:** le modèle prévoit qu'en principe, la décision quant aux entreprises tenues de déclarer les incidents reste du ressort des régulateurs sectoriels. De son côté, la centrale d'enregistrement des cyberincidents édicte des prescriptions sur les incidents devant lui être signalés.
- **Effets sur les points de contact existants:** les points de contact sont maintenus. Les déclarations de cyberincidents faites directement à MELANI ou à un CERT sectoriel ne sont plus facultatives mais obligatoires. Les points de contact en cas de cyberincident seraient ainsi renforcés, mais il faudrait définir précisément leur relation avec les points de contact sectoriels.
- **Organisation des processus:** il convient de distinguer au niveau des procédures entre les incidents physiques et les cyberincidents, en sachant qu'une distinction claire n'est pas simple dans tous les cas. Il serait avantageux de prévoir des délais d'annonce différents et d'ajuster les sanctions en fonction des cas. Il serait aussi possible de signaler les cyberincidents sous forme anonymisée à la centrale d'enregistrement.

5.4 Absence d’extension des obligations de déclarer en vigueur

Description: rien ne change dans le système en place, et les obligations de déclarer ne sont pas étendues. En particulier, il n’existe aucune obligation de déclarer les cyberincidents.
Avantages: l’échange volontaire d’informations, comme celui instauré par MELANI pour les cyberincidents, permet aux entreprises de signaler des incidents sans bureaucratie ni vérifications juridiques préalables. Comme une telle solution est bien acceptée des entreprises, les informations non soumises à l’obligation de déclarer ont de meilleures chances d’être partagées.
Inconvénients: il est impossible de dresser un tableau complet de la situation, et donc de procéder à des analyses statistiques. En renonçant à toute obligation de déclarer, le droit suisse ne serait pas compatible avec les prescriptions de la directive SRI en vigueur dans les États membres de l’UE.

6 Perspectives et prochaines étapes

Les modèles de base présentés seront approfondis avec des représentants des milieux économiques et des cantons, avec les régulateurs compétents et le monde politique. Il s’agira également d’examiner en détail les mesures législatives nécessaires pour chaque modèle. Les discussions auront lieu au premier semestre 2020, sous la direction du délégué de la Confédération à la cybersécurité.
Le but est de parvenir à un consensus sur le modèle d’obligations de déclarer à introduire en Suisse, afin que la mise au point des bases légales correspondantes puisse débuter dès l’été 2020.