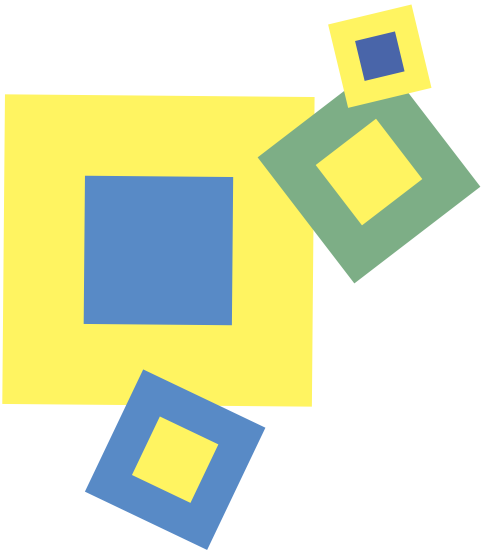
Recommandation législative

Une proposition pour améliorer la cybersécurité des infrastructures critiques en Suisse



Pourquoi cette recommandation législative ?

Il y a d'importantes lacunes en Suisse en matière de cybersécurité, même si un cadre légal est en développement. L'adoption, puis la révision, de la nouvelle Loi sur la sécurité de l'information (LSI) sont des pas importants, mais ce n'est pas suffisant pour assurer un niveau approprié de cyberrésilience en Suisse.

Ce document relève les lacunes légales les plus importantes en matière de cybersécurité des infrastructures critiques. Il propose des mesures législatives pouvant créer des incitations, plus précisément par l'introduction d'exigences minimales de cybersécurité pour les infrastructures critiques.

Ce document est le fruit d'un projet de recherche intitulé « Improving trust in cybersecurity through ethics and law » qui a été réalisé dans le cadre du programme national de recherche 77 « Transformation numérique » par des chercheurs de l'Université de Zurich et de l'Université de Lausanne avec le soutien du Centre national suisse pour la cybersécurité (NCSC).

Notions centrales et problématique

Qu'est-ce que la cybersécurité ?

La cybersécurité peut être définie comme l'ensemble des mesures visant à prévenir et gérer les cyberincidents ainsi qu'à améliorer la cyberrésilience[1].

La notion de cybersécurité peut être distinguée de la « sécurité de l'information » et de la « sécurité informatique ». Cela étant, les mesures de cybersécurité sont dans une large mesure similaires aux mesures permettant d'assurer la sécurité de l'information et la sécurité des moyens informatiques et peuvent donc être combinées avec celles-ci. Les trois notions sont étroitement liées.

La cybersécurité est un défi global qui ne peut être limité à des questions techniques. Elle implique au contraire différentes dimensions, dont la législation et la réglementation.

Historiquement, différents domaines juridiques ont été réglementés en tenant compte de considérations avoisinant la cybersécurité : le droit pénal vise par exemple la cybercriminalité, la cyberdéfense porte sur l'activité

1 Conseil fédéral, Cyberstratégie nationale (CSN), 2023, p. 9. La CSN a été adoptée en 2023, est la stratégie de protection de la Suisse contre les cybermenaces et remplace la Stratégie nationale pour la protection de la Suisse contre les cyberrisques (SNPC) 2018–2022.

77 PNR Transformation numérique Programme national de recherche

Universität Zürich[UZH]

UNIL | Université de Lausanne

militaire dans le cyberespace, et certains secteurs spécifiques de l'industrie adoptent des exigences de cybersécurité. Cette hétérogénéité rend difficile la réglementation de la cybersécurité.

Que sont les infrastructures critiques ?

Les infrastructures critiques sont des installations, processus et systèmes essentiels au fonctionnement de l'économie et au bien-être de la population (art. 5 lit. c LSI). L'art. 5 lit. c LSI fournit quelques exemples, tels que « l'approvisionnement en eau potable et en énergie, les infrastructures d'information, de communication et de transports ». Il n'existe pas de définition légale plus précise de la notion d'infrastructure critique.

Les infrastructures critiques comptent les organisations nécessaires à l'économie nationale et au bien-être de la population. La Stratégie nationale de protection des infrastructures critiques considère comme étant des infrastructures critiques tous les « éléments » qui fournissent des prestations dans l'un des vingt-sept sous-secteurs critiques composant les neuf secteurs critiques reconnus en Suisse, bien que la LSI ne le précise pas[2]. Cela inclut des petites, moyennes et grandes entreprises ainsi que des autorités et organisations étatiques.

Pourquoi est-ce important de réglementer la cybersécurité des infrastructures critiques ?

Il n'y a actuellement pas de loi générale sur la cybersécurité pour la société dans son ensemble, en raison des différents domaines juridiques concernés, des différents enjeux et des différentes pratiques. Alors qu'une telle loi serait difficile à concevoir, une loi sur la cybersécurité des infrastructures critiques est envisageable. La réglementation est une incitation nécessaire pour améliorer la cyberrésilience des infrastructures critiques.

Un cadre légal est en développement en Suisse pour encourager les infrastructures critiques à assurer un niveau adéquat de cybersécurité et à disposer de compétences de gestion de cyberincidents. Toutefois, ces efforts sont insuffisants et des lacunes légales demeurent. Il est nécessaire d'adapter la loi. De nombreuses infrastructures critiques ne sont pas soumises à des exigences minimales. En outre, il est difficile pour de nombreuses organisations de savoir si elles sont des infrastructures critiques, si elles sont soumises à des exigences et le cas échéant auxquelles, ce qui est problématique.

2 Les neuf secteurs comptent les autorités, l'énergie, l'élimination, les finances, la santé, l'information et la communication, l'alimentation, la sécurité publique et les transports, cf. Conseil fédéral, Stratégie nationale de protection des infrastructures critiques du 16 juin 2023 (FF2023 1659, p. 7).

Un cadre légal en cours de développement

Le cadre légal actuel pour la cybersécurité des infrastructures critiques

La cybersécurité est un domaine émergeant qui n'a donné lieu à des efforts législatifs que récemment.

La loi la plus importante est la LSI, qui entre en vigueur dans sa globalité et avec ses ordonnances le 1er janvier 2024. La LSI introduit en particulier des exigences minimales pour la sécurité de l'information et pour la sécurité des moyens informatiques des autorités et organisations de la Confédération. Les dispositions de la LSI imposent à ces dernières de mettre en place des mesures techniques et organisationnelles pour améliorer leur cybersécurité.

Une révision de la LSI a récemment été adoptée pour y introduire une obligation de signaler les cyberattaques ciblant les infrastructures critiques. La loi révisée (LSI2) devrait entrer en vigueur en 2025.

Bien que la LSI représente un pas important, elle est encore trop limitée. De nombreuses autres infrastructures critiques pourraient bénéficier des mesures imposées par la LSI.

En parallèle de la LSI, certains sous-secteurs critiques, comme celui de l'approvisionnement en électricité, révisent actuellement leur législation afin d'introduire des exigences minimales de cybersécurité contraignantes. Des bases légales manquant pour améliorer la cyberrésilience des infrastructures critiques de l'approvisionnement en électricité, la Loi sur l'approvisionnement en électricité (LApEl) et son ordonnance sont actuellement en voie de modification.

En outre, des dispositions légales sur les secrets (p. ex. sur les secrets commerciaux) ou sur la protection des données existent et prévoient des considérations liées à la cybersécurité des infrastructures critiques et plus largement. Fait notamment partie de ces lois la Loi sur la protection des données (LPD).

Finalement, des dispositions légales relatives à la responsabilité contractuelle, civile, administrative ou pénale permettent de réparer, au moins *a posteriori*, certains manquements en matière de cybersécurité.

Les lacunes du cadre légal actuel

Premièrement, l'absence d'un niveau suffisant et harmonisé de cybersécurité doit être mise en lien avec la difficulté d'appréhender la notion d'infrastructure critique. En d'autres termes, il manque une définition juridique claire de cette notion.

Deuxièmement, de nombreuses infrastructures critiques ne disposent pas d'exigences minimales de cybersécurité ou elles n'ont que des exigences lacunaires. Par exemple :

1. Les hôpitaux sont soumis à l'obligation de signaler les cyberattaques. Ils sont soumis à des obligations de cybersécurité dans des circonstances particulières, typiquement lors de l'utilisation de dispositifs médicaux ou de l'exploitation du dossier électronique du patient. Autrement, ils ne sont soumis qu'à des recommandations. Seuls certains hôpitaux disposent de processus internes pour assurer la cybersécurité.
2. Les autorités communales sont soumises uniquement à l'obligation de signaler les cyberattaques. Autrement, leur situation dépend de chaque canton et des directives internes de chaque commune, ce que l'on peut percevoir comme des incitations insuffisantes.
3. Le sous-secteur critique des services informatiques couvre les services informatiques pour l'économie (en particulier le traitement et le stockage des données, les services de sécurité numérique ou les services infonuagiques). Les organisations actives dans ce sous-secteur ne sont aujourd'hui pas soumises à des exigences minimales de cybersécurité, que ce soit pour leurs ressources informatiques ou pour les services et produits qu'elles fournissent dans le cadre de leur activité. Les normes légales sur l'obligation de signaler les cyberattaques, sur la protection des données, sur la responsabilité contractuelle ou encore sur la sécurité s'appliquent mais ont un champ limité et sont des normes réactives et non proactives.

Troisièmement, nous constatons non seulement d'importantes lacunes dans la réglementation de la cybersécurité au sein de nombreuses infrastructures critiques, mais également des organisations (soumises ou non à des exigences minimales de cybersécurité) perdues dans la diversité des dispositions leur étant applicables. Les normes sont dispersées et les infrastructures critiques ne sont pas toutes soumises à une obligation de dresser une liste des normes leur étant applicables. Un manque de cohérence et de clarté dans le cadre juridique actuel est donc à déplorer.

La solution : des exigences minimales transversales

Des exigences minimales transversales et applicables à l'ensemble des infrastructures critiques sont aujourd'hui nécessaires. Il faut passer par une loi générale

Nous plaidons pour l'introduction d'exigences minimales applicables à toutes les infrastructures critiques. Il est important que l'ensemble des infrastructures critiques améliorent leur cyberrésilience. Le meilleur moyen d'atteindre ce niveau harmonisé est l'application d'exigences minimales de cybersécurité à l'ensemble de ces organisations (exception faite des moins importantes)[3] .

Les raisons justifiant une législation générale sont les suivantes.

- Une base légale générale permet d'identifier qui est une infrastructure critique et quelles exigences minimales s'appliquent.
- Une loi générale entrerait en vigueur plus rapidement pour l'ensemble des infrastructures critiques, permettant une meilleure anticipation et une meilleure capacité d'adaptation dans le temps face aux évolutions technologiques.
- Des exigences uniformes permettent de mutualiser les efforts et réaliser des économies.
- Une loi générale rend plus difficile pour certaines infrastructures critiques de passer entre les mailles du filet.
- Une loi générale et uniforme peut facilement servir de modèle pour l'économie privée qui pourrait s'en inspirer.

La Loi sur la sécurité de l'information (LSI) comme loi adéquate pour l'ensemble des infrastructures critiques

La LSI est la loi principale pour la cybersécurité en Suisse. L'adoption de la LSI et sa révision constituent des étapes importantes pour la cybersécurité en Suisse. La LSI sert déjà de fondement pour les exigences minimales pour la sécurité de l'information et la sécurité des moyens informatiques des autorités et organisations de la Confédération. Elle servira également de base juridique à l'obligation de signaler les cyberattaques visant

3 En opposition à ce que préconise la CSN, à savoir l'examen en continu des besoins légaux et de l'adaptation du cadre légal, Conseil fédéral, CSN, 2023, p. 21.

les infrastructures critiques.

La LSI est donc adéquate, si ce n'est idéale, pour introduire les exigences minimales de cybersécurité applicable à l'ensemble des infrastructures critiques.

Notre recommandation législative

Notre recommandation pour des exigences minimales de cybersécurité des infrastructures critiques

Notre recommandation consiste en trois améliorations de la LSI :

1. ***La notion d'infrastructure critique doit être clarifiée et le champ d'application des exigences minimales de la LSI doit être étendu. Il ne doit pas se limiter aux autorités et organisations de la Confédération, mais s'appliquer aux autres infrastructures critiques.***

La notion d'infrastructure critique doit être précisée par rapport à ce que l'art. 5 lit. c LSI prévoit actuellement. La loi peut prendre comme inspiration l'indication de la Stratégie de protection des infrastructures critiques pour préciser que les infrastructures critiques sont, en plus d'être nécessaires à l'économie nationale et au bien-être de la population, tous les éléments qui fournissent des prestations importantes dans l'un des sous-secteurs critiques.

Le champ d'application des exigences minimales dépend de la définition d'infrastructures critiques. L'on pourrait concevoir un champ d'application similaire à ce qui existe aux art. 74b s. LSI2, ou une obligation générale à toute infrastructure critique de respecter les exigences minimales avec une exception consistant en la possibilité pour le Conseil fédéral d'exempter certaines organisations (typiquement en raison d'une moindre importance pour l'économie ou le bien-être de la population), comme cela existe déjà à l'art. 74c LSI2.

2. ***Les exigences minimales de la LSI doivent être renforcées.***

Les mesures imposées par la LSI et son ordonnance couvrent déjà certains besoins. Pour le surplus, on peut envisager les mesures suivantes : l'élaboration de plans de gestion de cyberincidents, d'inventaires des objets à protéger ou des normes plus largement applicables en matière de cybersécurité, ou encore des obligations de cybersécurité par défaut et dès la conception.

3. ***Les services informatiques, en particulier les services numériques de sécurité dont font partie les équipes de gestion de cyberincidents (Computer Security Incident Response Teams, CSIRTs), doivent être soumis à des exigences spécifiques supplémentaires.***

Les CSIRTs et les services informatiques en général doivent non seulement garantir la cybersécurité des informations qu'ils traitent ou des outils informatiques qu'ils exploitent, mais aussi celle des produits et services qu'ils proposent.

Cette obligation doit se matérialiser par une garantie de capacités et de compétences suffisantes (notamment personnelles ou financières). Il devrait également y avoir une obligation d'assurer la cybersécurité à chaque étape de la chaîne d'approvisionnement d'un produit ou d'un service. En outre, une obligation de transparence devrait exister en termes de qualité et de sécurité des services fournis.

La loi doit laisser de la place aux actes d'exécution

Des actes d'exécution sous forme des ordonnances, des actes de droit souple (soft law) et des prescriptions techniques et administratives doivent pouvoir être adoptés. Ceux-ci peuvent être plus précis et adaptés plus rapidement qu'une loi. Ils peuvent impliquer des autorités qui disposent de compétences plus poussées (Conseil fédéral, Office fédéral de la cybersécurité (OFCS), service spécialisé de la Confédération pour la sécurité de l'information[4], autorités sectorielles et associations professionnelles).

Le nouvel OFCS doit continuer de détenir des compétences pour la cybersécurité des infrastructures critiques. Le nouveau service spécialisé de la Confédération pour la sécurité de l'information disposera vraisemblablement des compétences pour adopter des directives (principalement à l'attention de la Confédération) et il conviendra de voir comment ces compétences s'organisent entre les deux autorités. L'OFCS doit par exemple pouvoir adopter des directives et des lignes directrices (comme la directive Si001 à l'attention de la Confédération, mais pour les autres infrastructures critiques). Dans tous les cas, les mesures concrètes que les infrastructures critiques doivent prendre doivent souvent figurer dans des actes d'exécution plutôt que dans la loi.

4 Le service spécialisé de la Confédération pour la sécurité de l'information est créé avec l'entrée en vigueur de la LSI au 1er janvier 2024. Il fait partie du Secrétariat d'État à la politique de sécurité (SEPOS) du Département fédéral de la défense, de la protection de la population et des sports (DDPS). Ses tâches sont décrites à l'art. 83 LSI et dans différentes dispositions de l'OSI ; pour de plus amples informations, https://www.sepos.admin.ch/fr.

Les autorités sectorielles et les associations professionnelles connaissent particulièrement bien les infrastructures critiques actives dans les sous-secteurs spécifiques. L'adoption d'exigences minimales pour l'ensemble des infrastructures critiques dans une loi générale (LSI) ne doit pas empêcher l'adoption d'actes d'exécution sectoriels qui tiennent compte des caractéristiques ou des particularités propres à chaque secteur et liées à l'utilisation de technologies spécifiques. Par exemple, différents secteurs de l'approvisionnement économique du pays ont élaboré des lignes directrices et des recommandations pour la résilience informatique en tenant compte de certains outils spécifiques (comme les compteurs intelligents), sur la base de la norme minimale pour les TIC adoptée par l'Office fédéral pour l'approvisionnement économique du pays (OFAE).

Finalement, les cantons doivent aussi pouvoir imposer des exigences supplémentaires aux infrastructures cantonales. C'est une expression du principe de subsidiarité.

Le rôle du nouvel OFCS doit être renforcé

Bien que la répartition des compétences entre l'OFCS et le service spécialisé de la Confédération pour la sécurité de l'information soit incertaine, l'OFCS doit conserver ses compétences en ce qui concerne la cybersécurité des infrastructures critiques. Les autorités et organisations de la Confédération faisant partie des infrastructures critiques, nous regrettons la décision de transférer dans les années à venir de nombreuses compétences concernant leur cybersécurité au service spécialisé de la Confédération pour la sécurité de l'information.

Le futur office devrait coordonner la mise en œuvre des exigences minimales. Il devrait en outre pouvoir soutenir l'ensemble des infrastructures critiques, par exemple par la mise à disposition d'informations techniques sur les cybermenaces en cours ou de recommandations sur des mesures préventives et réactives (art. 74 LSI).

Il joue un rôle clé pour mettre en œuvre et surveiller l'application de la loi comme de notre recommandation. Il dispose déjà de compétences de surveillance en relation avec l'obligation de signaler les cyberattaques. Il serait judicieux que le rôle de l'OFCS soit renforcé et qu'il puisse effectuer divers actes de surveillance (comme la réalisation d'inspections ou d'audits, l'accès à l'information ou l'émission d'avertissements). La mise en œuvre de la loi nécessitera également des ressources (humaines, financières, etc.) de la Confédération.

Des sanctions sont nécessaires en cas de violation de la LSI. Celles-ci permettront d'encourager les organisations à respecter les exigences minimales, comme ce sera déjà le cas pour l'obligation d'annoncer les cyberattaques. Il est possible de maintenir un processus en plusieurs étapes (avec une information et un avertissement de l'OFCS, avant une décision et l'initiation d'un réel processus de sanction, à l'instar du système des art. 74g let. h LSI2). Ce mécanisme permettrait de conserver la confiance des infrastructures critiques vis-à-vis de l'OFCS.

Nous sommes convaincus que la réglementation de la cybersécurité aura un effet très positif sur la réduction des cybermenaces en Suisse. Elle contribue à renforcer l'autonomie et la responsabilité individuelle des infrastructures critiques. La cybersécurité est toujours un effort collectif de tous les acteurs impliqués.

Notre recommandation en trois étapes

1. **Redéfinir la notion d'infrastructure critique et étendre le champ d'application des exigences minimales de cybersécurité de la LSI.**
2. **Renforcer les exigences minimales existantes.**
3. **Introduire des exigences légales supplémentaires pour les services informatiques, en particulier pour les services numériques de sécurité.**

Responsables de l'édition

Rédaction
Pauline Meyer, Sylvain Métille

Chercheurs
Markus Christen, Melanie Knieps, *Digital Society Initiative, Universität Zürich.*
David-Olivier Jaquet-Chiffelle, Sylvain Métille, Pauline Meyer, Delphine Sarrasin, *Faculté de droit, des sciences criminelles, et d'administration publique, Université de Lausanne*.
Reto Inversini, *Nationales Zentrum für Cybersicherheit.*

Conception
Rosa Guggenheim, guggenheim.li

Contact pour les questions
christen@ethik.uzh.ch, pauline.meyer@unil.ch

Le document est disponible en français et allemand.