Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Le Conseil fédéral

Berne, le 15.12.2023

Infrastructure numérique. Réduire les risques géopolitiques

Rapport du Conseil fédéral donnant suite au postulat 20.3984 Pult du 14.9.2020

Synthèse

Le postulat Pult 20.3984 charge le Conseil fédéral de présenter un rapport sur les moyens de réduire les risques géopolitiques liés aux infrastructures numériques comme la 5G et à des fournisseurs d'équipements comme le chinois *Huawei*.

La Suisse court incontestablement des risques techniques à composante géopolitique du fait que nombre de nos processus économiques, sociaux ou politiques sont gérés par des réseaux et systèmes numériques qui peuvent présenter des failles de sécurité ou faire l'objet de cyberattaques. Dans le contexte géopolitique mondial clivant qui se met en place, la Suisse court par ailleurs des risques géopolitiques potentiels (par ex. une mesure de blocage de l'accès à son marché par l'UE) en lien avec des infrastructures numériques et de télécommunication provenant de fournisseurs jugés à risques ou qui sont contrôlés par un Etat présentant un risque géopolitique.

Afin de renforcer la résilience de nos télécommunications, le Conseil fédéral propose de nouvelles mesures qui portent sur une stratégie «multifournisseurs», les équipements jugés à risque et la prochaine mise au concours de fréquences. Pour le reste, l'écosystème suisse de la cybersécurité devrait être à même de fournir à terme les organismes nationaux de contrôle et de certification dont notre pays a besoin.

A l'instar de ce qui est envisagé par l'UE dans la boîte à outils 5G et dans d'autres projets de réglementation notamment sur la cyber-résilience, le Conseil fédéral estime nécessaire de prévoir dans la loi sur les télécommunications (LTC; RS 784.10) une nouvelle disposition lui donnant la possibilité de prendre les mesures qui s'imposent lorsqu'un risque géopolitique se matérialise. Il s'agit en particulier de lui permettre d'interdire l'acquisition, la mise en place et l'exploitation d'équipements provenant de fournisseurs jugés problématiques pour la sécurité de notre pays ou qui sont détenus, contrôlés ou sous l'influence d'un Etat étranger présentant un risque géopolitique pour la Suisse. A cet égard, la liberté économique et le bon fonctionnement de la concurrence doivent être garantis dans la mesure du possible.

Une collaboration internationale demeure indispensable afin de garantir la sécurité des réseaux et des infrastructures numériques compte tenu de leur interconnexion à l'échelle mondiale.

Table des matières

Abréviations

3GPP	The 3rd Generation Partnership Project
5G	Réseau ou communication mobile de 5ème génération
AGCS	Accord général sur le commerce des services (OMC)
ch.	chiffre
Cst.	Constitution fédérale de la Confédération suisse
CSN	Cyberstratégie nationale
CYD	Cyber Defense
DDoS	Déni de service distribué (Distributed Denial of Service attack)
DFAE	Département fédéral des affaires étrangères
EMPA	Institut interdisciplinaire de recherche pour les sciences des matériaux et la technologie au sein du Domaine des EPF
ENISA	Agence de l'UE pour la cybersécurité (European Union Agency for Cyber-security)
EPFZ	Ecole polytechnique fédérale de Zurich
ETSI	European Telecommunications Standards Institute (Institut européen de standardisation des télécommunications)
FIRST	Forum of Incident Response and Security Teams
GATT	Accord général sur les tarifs douaniers et le commerce (General Agreement on Tariffs and Trade) (OMC)
GSMA	The GSM Association
LSI	Loi fédérale sur la sécurité de l'information au sein de la Confédération
LTC	Loi sur les télécommunications
NatCSIRT	National Computer Security Incident Response Team
NCSC	Centre national pour la cybersécurité (National Cyber Security Center)
NESAS	Network Equipment Security Assurance Scheme
NOC	Centre des opérations du réseau (Network Operation Center)
NTC	Institut national de test pour la cybersécurité (Nationale Testinstitut für Cybersicherheit)
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFCOM	Office fédéral de la télécommunication
OMC	Organisation mondiale du commerce
ONU	Organisation des Nations Unies
OOIT	Ordonnance de l'OFCOM sur les installations de télécommunication
O-RAN	Open Radio Access Network
OSCE	Organisation pour la sécurité de la coopération en Europe
OST	Ordonnance sur les services de télécommunication
OTC	Accord sur les obstacles techniques au commerce (OMC)
RAN	Réseau d'accès radio (Radio Access Network)
SCION	Scalability, Control, and Isolation on Next-Generation Networks
SGSI	Système de gestion de la sécurité de l'information
SOC	Centres de gestion de la sécurité (Security Operation Center)
SRC	Service de renseignement de la Confédération
SSFN	Secure Swiss Finance Network
TF-CSIRT	Task Force Computer Security Incident Response Team
TIC	Technologies de l'information et de la communication
UE	Union européenne
UIT	Union internationale des télécommunications

1 Le postulat 20.3984

Conformément au postulat Pult 20.3984 du 14 septembre 2020 qui a été adopté le 17 juin 2021 par le Conseil national, le Conseil fédéral est chargé de présenter un rapport dans lequel il expose les moyens qui permettraient de réduire les risques géopolitiques qui accompagnent la généralisation et le développement d'infrastructures numériques comme la 5G. Le choix des fournisseurs de technologie devra tenir compte de la qualité des produits, de la fiabilité des chaînes d'approvisionnement, de la structure sociale des fournisseurs et du cadre juridique auquel le siège de l'entreprise est soumis. Il sera plus particulièrement nécessaire de préciser les risques qui émanent de prestataires tels que Huawei, domiciliés dans des pays qui ne sont ni des économies de marché ni des États de droit. Enfin, il s'agira de répondre à la question de savoir comment garantir que l'infrastructure technologique de la Suisse ne sera pas affectée par l'affrontement géoéconomique qui opposera dans un avenir prévisible les États-Unis et la Chine.

Le postulat s’insère dans un ensemble d’interpellations parlementaires qui questionnent les risques géopolitiques encourus par la Suisse en matière de chaînes d’approvisionnement et d’infrastructures. Un rapport du Conseil fédéral du 24 novembre 2021 concernant la sécurité des produits et la gestion des risques de la chaîne d’approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense répond aux postulats Dobler 19.3135 et 19.3136. Donnant suite à la motion 20.3268 Häberli-Koller, le Conseil fédéral a en outre publié le 31 août 2022 un rapport sur le rôle des chaînes de valeur mondiales dans la sécurité de l’approvisionnement de la Suisse en biens essentiels.

La motion Groupe socialiste 22.3414 «Protection des infrastructures critiques de la Suisse contre l'influence d'autres États» a été adoptée le 2 mai 2023 par le Conseil national et suspendue le 3 juillet 2023 par la Commission de la politique de sécurité du Conseil des Etats dans l’attente du rapport du Conseil fédéral donnant suite au présent Postulat Pult 20.3984. Par ailleurs, le Conseil fédéral adoptera d'ici fin 2024 un rapport en réponse au postulat Z'graggen 22.4411 «Stratégie Souveraineté numérique de la Suisse». Il y définira la notion de «souveraineté numérique», évaluera le degré de cette souveraineté pour la Suisse et proposera les mesures nécessaires en la matière.

2 L’infrastructure suisse de télécommunication

2.1 Un état des lieux de la 5G

Les opérateurs de radiocommunication *Salt*, *Sunrise* et *Swisscom* exploitent des réseaux de téléphonie mobile de 5ème génération (5G) en Suisse pour offrir des services de télécommunication. Les équipementiers qui leur fournissent du matériel 5G sont en définitive nombreux et proviennent de différents horizons: *Ericsson* (SE), *Nokia* (FIN) *Huawei* (CN), *Microsoft* (*eSPIN & Services*) (UK), *A10 Networks* (USA), *Cisco* (USA), *Juniper* (USA), *Commscope* (USA) et *Ceragon* (ISR).

Le cœur de réseau (Core Network) est un élément essentiel d’un réseau 5G. Il est composé des fonctionnalités principales suivantes: gestion des accès et de leur sécu-

rité, authentification des abonnés, acheminement des appels et des données, gestion des services d'abonnés, contrôle des flux et de leur priorisation, gestion de l'interfonctionnement avec les autres réseaux, contrôle de la communication pendant toute la durée des transmissions assurant leur continuité notamment lors des déplacements des usagers (handover) et gestion de la qualité de service et de la facturation. Un seul opérateur suit une stratégie «multifournisseurs» pour ce qui est du cœur de réseau. Les deux autres opérateurs utilisent exclusivement les équipements d'un seul fournisseur, soit de *Huawei* à 100% soit de *Nokia* à 100%.

Le réseau d'accès radio (Radio Access Network, RAN) d'un réseau mobile connecte les appareils des utilisateurs finaux, leurs smartphones par exemple, à un service de stockage en nuage (cloud). Il transmet les informations par ondes radio, d'abord depuis les appareils des utilisateurs finaux vers les émetteurs-récepteurs RAN, puis de ces derniers vers le cœur de réseau qui est lui-même connecté à Internet ou à d'autres opérateurs. Les réseaux RAN effectuent des tâches complexes de traitement des connexions et leur développement repose de plus en plus sur la virtualisation de leurs fonctions. Pour ce qui est des réseaux RAN utilisés en Suisse, un des opérateurs utilise les équipements de *Huawei* à 100%, un autre ceux de *Huawei* à 80% et de *Nokia* à 20% et le dernier ceux de *Ericsson* à presque 100%[1].

Le terme «backhaul» désigne, dans les réseaux de téléphonie mobile, le réseau de transmission et les liens entre le cœur de réseau et les antennes relais du réseau d'accès radio (RAN). Les liaisons composant un réseau «backhaul» peuvent être en fibres optiques, en cuivre ou effectuées par des faisceaux hertziens. Le réseau de transmission (backhaul) est composé d'équipements provenant de fournisseurs américains et de *Ericsson* pour un opérateur, de *Huawei*, *Ericsson* et *Nokia* pour le deuxième et de *Huawei* uniquement pour le troisième.

En ce qui concerne les interfaces vers les autres opérateurs ou services (par ex. l'interconnexion avec un autre opérateur, les opérations de maintenance, la facturation, l'accès Internet), un opérateur utilise les équipements de *Cisco* et de *Ericsson*, un autre ceux de *Cisco* et *Huawei* et le dernier ceux de *Huawei* uniquement.

Une analyse globale des équipements utilisés dans les réseaux 5G en Suisse permet de conclure qu'un seul des 3 opérateurs mobiles suisses est extrêmement dépendant de l'équipementier chinois *Huawei* pour ses fournitures. Dans la mesure où l'un des autres opérateurs recourt partiellement à des équipements *Huawei*, il convient de souligner ici que chaque élément de l'infrastructure 5G a accès à une part importante de l'infrastructure globale contrairement aux générations précédentes de téléphonie mobile qui séparaient infrastructure périphérique et centrale. Ce qui signifie que toute vulnérabilité ou porte dérobée dans un équipement 5G peut potentiellement compromettre tout le réseau 5G (cf. ch. 2.2 sur les risques techniques).

[1] L'Open RAN Alliance (O-RAN Alliance) a pour objectif d'améliorer l'interopérabilité future des différents composants d'un réseau d'accès radio. En standardisant les interfaces, la norme Open RAN doit permettre d'utiliser dans un réseau de téléphonie mobile des composants matériels et logiciels de différents fabricants sans devoir procéder à des adaptations.

Les centres opérationnels des opérateurs constituent des infrastructures centralisées essentielles pour les réseaux de télécommunication, dont la localisation géographique participe à la sécurisation des réseaux 5G (cf. ch. 4.1). Le centre des opérations du réseau (Network Operation Center, NOC) surveille et gère les performances et la disponibilité d'un réseau de télécommunication, alors que le centre de gestion de la sécurité (Security Operation Center, SOC) collecte, analyse et répond aux alertes de sécurité et aux cybers incidents. Ce dernier utilise des outils avancés de détection des menaces et de gestion des événements de sécurité qui identifient les activités suspectes, les vulnérabilités et les tentatives d'intrusion ou d'attaques.

2.2 Les risques techniques à composante géopolitique

La numérisation a pour conséquence que de plus en plus de processus économiques, sociaux ou politiques sensibles pour un Etat sont gérés par des réseaux et des système numériques qui peuvent faire l'objet de cyberattaques. Celles-ci sont menées de manière professionnelle par des acteurs étatiques, semi-étatiques ou non étatiques qui se servent de vulnérabilités et de failles de sécurité au sein des systèmes informatiques et de télécommunication, ou qui recourent à des logiciels malveillants (chevaux de Troie, espions logiciels et autres «malware») ou à des portes dérobées préinstallées («back doors») permettant de contrôler ou de faire dysfonctionner les systèmes infectés.

Les cyberattaques représentent des risques géopolitiques qui peuvent être lourds de conséquences pour un pays comme la Suisse. En particulier, la mise en réseau et la complexité croissante des infrastructures et des systèmes numériques fournissent aux auteurs de cyberattaques des moyens de pirater et de saboter le fonctionnement de nos infrastructures sensibles ou critiques. Cela peut concrètement toucher en particulier les réseaux d'énergie, les services financiers ou encore les réseaux d'approvisionnement en eau, avec des répercussions tant économiques que politiques sur l'Etat, les entreprises et les citoyens. Par ailleurs, des moyens cybers considérables sont déployés à travers le monde aux fins d'espionnage. La Suisse n'y échappe pas en tant que territoire intéressant pour les services de renseignement étrangers en raison de ses performances économiques et scientifiques, de la présence sur son sol d'une multitude d'organisations internationales et des nombreuses conférences internationales qu'elle accueille[2].

La Suisse a déjà subi des cyberattaques contre ses infrastructures numériques menées pour certaines probablement par des pays étrangers même si leur origine est demeurée incertaine, notamment contre l'entreprise RUAG (2014–2016), le Département fédéral des affaires étrangères DFAE (2017), le Laboratoire de Spiez en matière de menaces atomiques, biologiques et chimiques (2018), l'Organisation des Nations Unies ONU à Genève (2020) ou dernièrement le réseau d'entreprise des CFF, l'Université de Zurich et l'Administration fédérale au travers de l'entreprise suisse *Xplain* (2023). Une attaque générale DDoS du groupe pro-russe *NoName* en réaction au discours du président ukrainien devant les Chambres fédérales a par ailleurs touché en

[2] Rapport du Conseil fédéral du 12 mai 2023 aux Chambres fédérales et au public: Appréciation annuelle de la menace, p. 8.

juin 2023 les sites web du Parlement, de l'Administration fédérale, de la Poste, de l'Aéroport de Genève, de l'Armée, de cantons et de villes suisses.

A l'instar du *Cloud Act* états-unien, une loi chinoise de 2017 oblige les entreprises chinoises à collaborer et à partager avec les services de renseignement de leur pays l'accès aux données qu'elles récoltent, y compris pour leurs opérations à l'étranger. L'entreprise *Huawei*, qui a été fondée en 1987 par un ancien haut responsable de l'armée chinoise et qui a bénéficié d'un large soutien financier de l'Etat, est accusée par les Etats-Unis d'espionnage pour le compte des autorités chinoises. Si aucune preuve d'une activité d'espionnage ou de l'installation de portes dérobées dans les infrastructures 5G par *Huawei* n'a été publiquement apportée à ce jour, certaines attaques ou portes dérobées demeurent difficiles voire impossibles à détecter. Il est par ailleurs tout à fait envisageable pour un fournisseur d'équipements d'installer ultérieurement des mises à jour logicielles délibérément modifiées[3].

2.3 Les risques géopolitiques proprement dits

Les crises actuelles (notamment pandémie de COVID-19, guerre en Ukraine, changement climatique, crise énergétique, insécurités économiques et tensions au sujet de Taïwan) mettent en évidence des clivages géopolitiques croissants au niveau mondial[4]. Ces clivages se répercutent sur le développement technologique et l'innovation et pourraient réduire la disponibilité des biens de haute technologie. Les tensions grandissantes entre la Chine et les États-Unis dans le domaine de la sécurité nationale et de la technologie pourraient notamment provoquer des ruptures dans les chaînes d'approvisionnement de biens stratégiques comme les équipements de télécommunication, menacer l'interconnexion des marchés voire entraîner leur découplage. Au vu de l'intensification de la concurrence internationale en matière d'influence dans le cyberespace, les risques d'ingérences directes des États sur les fournisseurs d'équipements ont augmenté[5].

Le clivage avec l'Occident se concrétise dans la volonté affichée par des pays tels que la Chine, la Russie et un nombre croissant de pays du Sud global d'avoir plus d'influence sur un ordre mondial perçu comme trop «occidental», ce qui pose un défi pour la Suisse en termes de positionnement politique et économique. Ce défi du positionnement peut mettre en péril les facteurs qui ont fait le succès de notre pays, à savoir son ouverture libre-échangiste sur le monde et sa capacité d'innovation qui dépend de l'accès de nos entreprises à tous les produits et services technologiques de pointe de par le monde. L'approche pragmatique en matière de politique étrangère de la Suisse doit nous aider à concilier ces tensions et à maintenir une approche suisse

[3] Il convient de signaler que *Huawei* met en œuvre des standards de sécurité reconnus tel NESAS (Network Equipment Security Assurance Scheme), contribue aux travaux en matière de sécurité du GSMA (Global System for Mobile Communications Association) et offre à tous ses clients la possibilité de consulter le code source des programmes, du système d'exploitation ou des applications qui se trouvent dans ses composants réseau.
[4] Sur la tendance à un monde de plus en plus bipolarisé, cf. Service de renseignement de la Confédération SRC, La Sécurité de la Suisse 2023 du 26 juin 2023, p.27 ss.
[5] Rapport du Conseil fédéral du 24 novembre 2021 concernant la sécurité des produits et la gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense, en réponse aux postulats Dobler 19.3135 et 19.3136, p. 8.

générale et non discriminante des risques sécuritaires liés aux infrastructures numériques.

S'il le faut, la Suisse devrait toutefois être prête à s'intégrer davantage au niveau international compte tenu de son système de valeurs fondé sur la liberté et l'état de droit et à rester partie intégrante du système d'innovation de l'hémisphère occidental. Il s'agirait d'éviter que notre pays ne soit considéré comme une faille sécuritaire au milieu de l'Europe[6], discriminé économiquement en cas d'utilisation de certaines infrastructures de réseau provenant de la Chine ou que ce pays puisse se servir de notre potentielle dépendance à son infrastructure numérique pour exercer des pressions d'ordre politique sur la Suisse. Il n'est en définitive pas exclu que la Suisse soit in fine contrainte de choisir dans des cas spécifiques entre soutenir les États-Unis et maintenir une position indépendante[7].

3 Le régime juridique et politique actuel

3.1 Obligations internationales

L'Accord général sur le commerce des services (AGCS)[8] réglemente le commerce international des services, y compris des services de télécommunication. L'AGCS est complété par les règles contraignantes contenues dans l'Annexe sur les télécommunications et le Quatrième protocole concernant l'Annexe sur les négociations sur les télécommunications qui incorpore les engagements spécifiques de chaque Etat membre (cf. art. XVI et XXIX AGCS). Au-delà du fait qu'elle s'est engagée sur la base de ces différents accords à libéraliser son marché des télécommunications, la Suisse est tenue de garantir aux prestataires de services et aux services de tout Membre de l'OMC un traitement non discriminatoire (clause de la nation la plus favorisée).

L'Accord général sur les tarifs douaniers et le commerce (GATT)[9] libéralise le commerce des marchandises sur la base des listes de concessions de chaque Membre, et s'applique le cas échéant aux installations et autres équipements de télécommunication. Le GATT est complété par l'accord sur les obstacles techniques au commerce (OTC)[10] qui fixe un cadre multilatéral visant notamment à garantir que les prescriptions techniques, normes et procédures d'évaluation de la conformité soient non discriminatoires et ne créent pas d'obstacles non nécessaires au commerce. L'accord OTC reconnait le droit d'édicter des prescriptions techniques fixant un niveau de protection approprié des objectifs légitimes comme la sécurité nationale dans le respect des principes de non-discrimination, de proportionnalité et de transparence.

---

[6] Dans son rapport du 9 juin 2023 sur l'état actuel des relations Suisse-UE p. 11, le Conseil fédéral souligne que l'UE observe avec inquiétude l'influence technologique grandissante de la Chine. Afin d'empêcher ou de réduire de futures dépendances, elle entend promouvoir les capacités de développement et de production au sein du marché intérieur (souveraineté technologique). Ce qui n'est pas sans répercussions sur les entreprises et les consommateurs en Suisse.

[7] Chancellerie fédérale, Suisse 2035- Les grands défis de demain en 20 questions - analyse de la situation et du contexte 2022, p. 69 et 72.

[8] L'AGCS fait partie de l'Accord du 15 avril 1994 instituant l'Organisation mondiale du commerce (OMC) (annexe 1.B; RS 0.632.20).

[9] Le GATT (General Agreement on Tariffs and Trade) fait partie de l'Accord du 15 avril 1994 instituant l'OMC (annexe 1.B; RS 0.632.20).

[10] L'OTC fait partie de l'Accord du 15 avril 1994 instituant l'OMC (annexe 1A.6; RS 0.632.20).

Des restrictions ou exclusions d'accès à notre marché pour des équipementiers jugés problématiques pour la sécurité de notre pays ou détenus, contrôlés ou sous l'influence d'un Etat étranger présentant un risque sécuritaire peuvent violer les obligations AGCS, GATT et OTC de la Suisse. L'AGCS et le GATT contiennent des clauses d'exceptions permettant de justifier à certaines conditions des mesures nécessaires à la protection de l'ordre public (art. XIV let. a AGCS) ou de la sécurité (art. XIV let. c iii et XIVbis AGCS, art. XXI GATT)[11]. Ces exceptions sont interprétées de manière stricte par les organes adjudicateurs de l'OMC. L'Accord OTC permet également de tenir compte de considérations relatives à la sécurité nationale (art. 2.10, 5.4 et 5.7 OTC). Nombre de pays occidentaux et de l'UE ont du reste déjà pris des mesures sécuritaires à l'égard d'équipementiers jugés problématiques (cf. ch. 3.6), dans le respect présumé des accords AGCS, GATT et OTC dont ils font aussi partie.

Dans la mesure où il définit les droits et les obligations d'un État neutre en cas de conflit armé international[12], le droit de la neutralité ne concerne pas la prise éventuelle par la Suisse de mesures contraignantes qui toucheraient à l'acquisition et au développement d'infrastructures numériques et de télécommunication comme la 5G.

3.2 Droit des télécommunications et sécurité des réseaux

Le droit des télécommunications organise l'offre des services et des installations de télécommunication en les soumettant à la concurrence conformément aux engagements internationaux pris par la Suisse dans le cadre de l'Organisation mondiale du commerce (OMC; cf. ch. 3.1). Ce droit n'accorde actuellement à la Confédération aucune influence sur l'acquisition d'équipements de réseau par les opérateurs qui sont libres de leurs choix.

Conformément au secret des télécommunications (art. 13 al. 2 Cst. et 43 LTC), les opérateurs garantissent la confidentialité et l'intégrité des informations que les usagers leur confient en vue d'un acheminement par les télécommunications. Cela oblige les opérateurs à sécuriser leurs infrastructures contre des accès non autorisés et autres cyberattaques. Les contours de cette obligation ne sont pas précisés par le droit des télécommunications, les opérateurs devant prendre les mesures techniquement réalisables à des conditions raisonnables compte tenu des risques sécuritaires.

Sur la base d'un nouvel art. 48*a* LTC adopté en 2021, le Conseil fédéral a pu adopter dans l'ordonnance sur les services de télécommunication (OST; RS 784.101.1) certaines mesures qui renforcent la sécurité des réseaux de télécommunication. Le système de notification des perturbations dans l'exploitation des télécommunications a été consolidé et les fournisseurs d'accès à Internet doivent lutter contre les attaques par déni de service distribué (DDoS), peuvent bloquer ou restreindre des accès à In-

[11] L'art. 5 let. e de l'Annexe sur les télécommunications complète ces sauvegardes en prévoyant que l'accès et le recours aux réseaux et services publics de transport de l'information peuvent faire l'objet des conditions nécessaires pour protéger l'intégrité technique de ces services et réseaux.
[12] La neutralité permanente est un instrument de la politique étrangère de la Suisse (art. 173 al. 1 let. a et 185 al. 1 de la Constitution fédérale de la Confédération suisse [Cst.; RS 101). Le droit de la neutralité est codifié dans les Conventions de La Haye du 18 octobre 1907 (RS 0.515.21 et 0.515.22) et fait partie du droit international coutumier.

ternet ou des ressources d'adressage qui menacent de compromettre le bon fonctionnement des installations de télécommunication et doivent exploiter un service spécialisé qui recueille les signalements de telles manipulations.

Pour ce qui est de la sécurité des réseaux 5G, les opérateurs sont tenus d'exploiter un système de gestion de la sécurité de l'information (SGSI) conformément aux normes reconnues et aux exigences de l'OFCOM. Ils doivent par ailleurs exploiter leurs centres des opérations du réseau (NOC) et leurs centres de gestion de la sécurité (SOC) exclusivement dans des Etats dont la législation garantit une protection adéquate des données, les bases légales actuelles ne permettant toutefois pas d'imposer leur exploitation exclusivement en Suisse.

Les opérateurs qui exploitent les réseaux 5G doivent finalement garantir que les installations de télécommunication critiques du point de vue de la sécurité qu'ils exploitent correspondent à l'état de la technique. L'OFCOM peut définir les installations concernées, au besoin en collaboration avec la branche. Cette obligation implique le développement d'une procédure de certification ou d'évaluation de conformité des équipements critiques dans les réseaux mobiles (cf. ch. 4.3). Il serait à cet égard judicieux d'harmoniser la réglementation suisse avec celle de l'UE compte tenu du poids du marché européen et des accords de reconnaissance mutuelle avec l'UE en matière d'installations de télécommunication. L'Agence de l'UE pour la cybersécurité (ENISA) prépare un schéma de certification cybersécurité de la 5G qui fait suite à l'adoption de la boîte à outils 5G. Il conviendra d'examiner la possibilité pour la Suisse d'utiliser ce schéma de certification qui devrait se fonder sur des normes reconnues, voire de formaliser la coopération avec cette agence.

3.3 Résilience des infrastructures critiques

La loi fédérale sur la sécurité de l'information au sein de la Confédération (LSI; RS 128) vise à garantir la sécurité du traitement des informations relevant de la compétence de la Confédération et la sécurité de ses moyens informatiques. Elle prévoit en particulier une évaluation du risque pour les entreprises qui exécutent des mandats publics sensibles pour la sécurité de la Confédération[13]. Cette loi, qui n'est pas encore entrée en vigueur, doit faire l'objet de modifications qui renforcent la résilience de la Suisse face aux cyberrisques. Il s'agit d'ancrer dans la loi les tâches et compétences du futur nouvel Office fédéral pour la cybersécurité (OFCS) et de prévoir l'obligation de signaler les cyberattaques contre les infrastructures critiques en tant que processus et systèmes essentiels au fonctionnement de l'économie et au bien-être de la population.

Si l'Office fédéral pour l'approvisionnement économique du pays (OFAE) a publié une norme minimale de protection des TIC contre les cyberrisques, la future LSI n'en impose pas le respect aux infrastructures critiques. L'Administration fédérale en tient toutefois compte, puisqu'elle doit veiller à ce que ses organes et ses systèmes pré-

[13] Cette évaluation vise à exclure les entreprises qui laissent supposer avec une probabilité élevée qu'elles exécuteront les mandats de manière inadéquate ou contraire aux prescriptions de sécurité. Cela peut être le cas si l'entreprise est contrôlée ou influencée par des Etats étrangers de manière incompatible avec les intérêts de la Suisse (art. 57 al. 2 let. b LSI).

sentent une résilience appropriée face aux cyberrisques (art. 6 LSI). L'OFCS devra fournir par ailleurs un appui subsidiaire aux exploitants d'infrastructures critiques (art. 74 LSI). Lorsque des systèmes et réseaux informatiques qui se trouvent à l'étranger sont utilisés pour attaquer des infrastructures critiques en Suisse, le Service de renseignement de la Confédération (SRC) peut les infiltrer afin de perturber, empêcher ou ralentir l'accès à des informations (art. 37 al. 1 de la loi fédérale sur le renseignement; RS 121).

Le projet de dispositions de la LSI et la nouvelle Stratégie nationale de protection des infrastructures critiques adoptée par le Conseil fédéral en date du 16 juin 2023[14] concrétisent la cyberstratégie nationale (CSN) en dictant des mesures qui renforcent la résilience des infrastructures critiques numériques. Il revient pour le reste au Conseil fédéral de vérifier quels domaines ont besoin au surplus d'être réglementés et de proposer au Parlement, si nécessaire et si la Confédération est compétente, des modèles de directives contraignantes pour l'application de standards dans les infrastructures critiques.

Le protocole SCION (Scalability, Control, and Isolation on Next-Generation Networks), développé par l'Ecole polytechnique fédérale de Zurich (EPFZ), est un excellent exemple de ce qui peut être envisagé pour sécuriser les infrastructures critiques. Il permet de créer une nouvelle architecture d'Internet qui offre les propriétés des réseaux fermés et privés sur l'infrastructure Internet publique. SCION augmente la sécurité de l'Internet en permettant à l'expéditeur de sélectionner les chemins de transmission et d'exercer ainsi le contrôle sur le flux des informations. Depuis juin 2022, la Banque nationale suisse (BNS) utilise SCION au sein du Secure Swiss Finance Network (SSFN) avec l'opérateur de la bourse suisse SIX Group, les opérateurs Swisscom et Sunrise ainsi que SWITCH qui gère le domaine Internet «.ch».

3.4 Sécurisation des installations de télécommunication et d'autres produits TIC

L'atténuation des cyberrisques passe par la sécurisation des équipements installations de télécommunication et autres produits TIC qui présentent toujours de nombreuses failles de sécurité en termes de confidentialité, d'intégrité, de disponibilité et de traçabilité des données. A cet égard, l'adoption et l'application de standards de sécurité pour ces équipements, installations et produits TIC et leur certification ou évaluation de conformité par des entités reconnues contribuent à améliorer leur sécurité et leur bonne intégration au sein des infrastructures numériques.

Les dispositions introduites en 2022 dans l'ordonnance de l'OFCOM sur les installations de télécommunication (OOIT; RS 784.101.21) renforcent la cybersécurité de certains appareils sans fil (smartphones, montres connectées, traceurs d'activité et jouets sans fil) disponibles sur le marché suisse. Ceux-ci doivent intégrer des fonctionnalités qui les empêchent de nuire aux réseaux de communication afin d'en renforcer la résilience. Ces dispositions de l'OOIT couvrent également les installations des réseaux 5G. Elles ont permis à la Suisse d'aligner sa législation à celle de l'UE (cf. ch. 3.6). Pour faciliter l'évaluation de la conformité des installations et leur mise

[14] FF 2023 1659.

sur le marché, les organismes de normalisation européens élaborent des normes harmonisées qui devraient être mises à disposition de l'industrie européenne et suisse.

Il serait judicieux que la législation suisse considère, par exemple dans la loi fédérale sur les entraves techniques au commerce (LETC; RS 946.51) ou dans la LSI (cf. ch. 3.3), les questions de cybersécurité des produits à composants numériques critiques en prévoyant des exigences pour les fabricants de ces produits à l'instar du projet UE sur la cyber-résilience (ch. 3.6).

3.5 Cyberstratégie nationale

Conformément à l'orientation stratégique de la législature 2023 à 2027, la Confédération anticipe les cyberrisques, soutient et prend à leur égard des mesures efficaces visant à protéger la population, l'économie et les infrastructures critiques[15]. Cette orientation stratégique s'est vue concrétisée dans la CSN d'avril 2023[16] qui vise à protéger la Suisse contre les cybermenaces.

La CSN détaille les principales cybermenaces qui sont la source de risques géopolitiques comme le cyberespionnage, le cybersabotage, la cybersubversion qui vise à saper le système politique d'un État et les cyberopérations dans des contextes de conflits armés (cf. ch. 2.2). Elle souligne que l'évolution de la cybermenace dépend largement des changements géopolitiques et des innovations technologiques, et qu'il faut s'attendre à des tensions croissantes entre les pays comptant parmi les principaux fabricants de matériel informatique et de logiciels. La CSN s'appuie sur une approche exhaustive basée sur les risques, qui a pour objectif d'améliorer la résilience de la Suisse face aux cybermenaces. Il convient selon la CSN de vérifier dans quels domaines une législation qui prévoit des normes ou des réglementations à respecter s'impose, ce à quoi s'attelle précisément le présent rapport.

3.6 Mesures adoptées à l'étranger

Les Etats-Unis ont interdit en mai 2019 les produits et services des entreprises chinoises *Huawei* et *ZTE* dans leurs systèmes de télécommunication. Cette interdiction a été étendue en 2022 à tous les produits télécoms et de vidéosurveillance chinois Au-delà du soupçon d'espionnage, cette interdiction repose aussi sur des considérations liées à la domination du marché de la technologie 5G par les entreprises chinoises et par le retard en la matière des compagnies américaines. D'autres pays ont emboité le pas aux Etats-Unis de par le monde, en particulier le Canada, le Royaume-Uni, le Japon et l'Australie.

Les Etats membres de l'UE ont quant à eux défini une approche globale des risques liés aux réseaux 5G sous la forme d'une boîte à outils adoptée en janvier 2020[17]. Les mesures qui y sont proposées visent principalement à renforcer les exigences de sécurité, à évaluer les profils de risque des fournisseurs d'équipements, à appliquer des

---

[15] Conseil fédéral, Lignes directrices et objectifs du programme de la législature 2023 à 2027 du 11 janvier 2023, Objectif 18.
[16] https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-94237.html.
[17] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures (https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures).

restrictions utiles aux fournisseurs considérés à haut risque y compris leur exclusion, et à mettre en place des stratégies pour assurer la diversification des fournisseurs d'équipements. Si la plupart des Etats membres de l'UE ont adopté dans leur législation une limitation et/ou une interdiction de recourir à des fournisseurs à haut risque pour construire l'infrastructure 5G nationale ou ses parties critiques comme les fonctions de cœur de réseau, seule une partie de ces Etats membres a effectivement utilisé ces prérogatives pour restreindre ou exclure des fournisseurs à haut risque. La Commission européenne estime que *Huawei* et *ZTE* présentent des risques sensiblement plus élevés que les autres fournisseurs de 5G, considère que les restrictions et exclusions qui leur sont appliquées par 10 États membres sont justifiées conformément à la boîte à outils 5G et encourage vivement les autres États membres et les opérateurs de télécommunication à prendre de telles mesures au vu du risque pour la sécurité collective de l'Union[18].

La directive 2014/53/UE sur les équipements radioélectriques (RED) sur laquelle la Suisse s'est alignée (cf. ch. 3.4) établit un cadre réglementaire pour la mise sur le marché des équipements radioélectriques comprenant des exigences techniques en faveur de la protection de la vie privée, des données personnelles et contre la fraude. L'UE a par ailleurs dévoilé un projet de réglementation sur la cyberrésilience[19], qui prévoit des obligations pour les fabricants de produits ayant des éléments numériques. Ces obligations portent en particulier sur la conception, le développement et la production de ces produits, la gestion de leur cycle de vie et le signalement de vulnérabilités. Les Etats-Unis imposent aussi aux fournisseurs la transparence sur les composants des logiciels vendus à l'administration (Software Bill of Materials) sur la base d'un «executive order» de mai 2021 pour l'amélioration de la cybersécurité.

3.7 Un bref bilan du régime juridique et politique actuel

Si la Suisse prend déjà certaines mesures afin de sécuriser son infrastructure numérique, des risques sécuritaires demeurent en lien avec l'infrastructure de télécommunication qui offre des opportunités de pirater ou de saboter nos infrastructures critiques et d'exercer sur notre pays des chantages tant économiques que politiques (cf. ch. 2.2). Compte tenu des risques géopolitiques que cela fait courir à notre pays, il convient de renforcer les moyens de lutter contre ces risques techniques dans une approche générale et non discriminante.

Dans le contexte géopolitique mondial clivant qui se met en place, le risque existe par ailleurs que notre pays soit considéré comme une faille sécuritaire au milieu de l'Europe et discriminé économiquement en cas d'utilisation de certaines infrastructures numérique ou de réseau, voire puisse faire l'objet de pressions d'ordre politique en cas de dépendance potentielle à un ou à des fournisseur(s) d'équipements particulier(s) (cf. ch. 2.3). La prise en compte de ces risques géopolitiques dans la LTC devient dans ces conditions primordiale et incontournable.

---

[18] Communication du 15 juin 2023 (https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox).

[19] Proposition de règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020 [COM(2022) 454 final — 2022/0272 (COD)].

4 Des mesures potentielles à envisager

4.1 Renforcer la lutte contre les risques techniques

Compte tenu des risque techniques à composante géopolitique (cf. ch. 2.2 et 3.7), il convient de préciser et d'élargir dans la LTC les compétences du Conseil fédéral permettant d'établir les nouveaux outils et exigences nécessaires afin de renforcer la sécurité de nos infrastructures de télécommunication, dans la ligne de ce qui est envisagé par l'UE dans la boîte à outils 5G et dans d'autres projets de réglementation notamment sur la cyber-résilience, à savoir:

- Obliger les opérateurs de télécommunication à acquérir et à exploiter des équipements, installations et logiciels liés à l'offre de services de télécommunication qui proviennent de divers fournisseurs (stratégie multifournisseurs);
- Etendre les exigences sécuritaires prévues par l'OST pour les réseaux 5G (cf. ch. 3.2) à l'ensemble des réseaux de télécommunication, en particulier l'obligation de garantir que les équipements, installations et logiciels critiques du point de vue de la sécurité correspondent à l'état de la technique et sont soumis à des procédures adéquates de certification en matière de cybersécurité;
- Prévoir des contraintes supplémentaires pour des équipements, installations et logiciels liés à l'offre de services de télécommunication qui seraient jugés à risque;
- Fixer des exigences sécuritaires renforcées en matière d'acquisition et d'exploitation d'équipements, d'installations et de logiciels pour la prochaine mise au concours en 2028 des fréquences de radiocommunication destinées à la téléphonie mobile (concessions);
- Etudier la possibilité d'imposer une obligation de localiser en Suisse, pour autant que les obligations internationales de la Suisse le permettent, les NOC et SOC, qui devraient être exploités par l'opérateur lui-même ou par un mandataire indépendant des fournisseurs d'équipements,

La mise en œuvre de ces nouvelles exigences permettant fin de renforcer la sécurité de nos infrastructures de télécommunication passe par un développement des capacités de certification et de contrôle techniques dans notre pays (cf. ch. 4.3) et par la mise sur pied d'une surveillance renforcée de l'OFCOM.

Au regard du coût technologique et du niveau d'innovation nécessaires pour développer des infrastructures numériques, il serait peu réaliste d'envisager une politique industrielle qui permettrait de réduire la dépendance technologique de notre pays vis-à-vis de fournisseurs d'équipements étrangers. En revanche, il n'est pas exclu que des solutions sécuritaires particulières puissent être développées en Suisse en relation avec des installations, logiciels ou services liés aux services de télécommunication. Dans ce contexte, il serait judicieux que la recherche et le développement de telles solutions sécuritaires suisses, à l'exemple du protocole SCION développé par l'EPFZ (cf. ch. 3.3), puissent être soutenues par les instruments de financement adéquats existants (Fonds national suisse, Innosuisse).

4.2 Anticiper les risques géopolitiques

Compte tenu des risques géopolitiques potentiels qu'elle court (cf. ch. 2.3 et 3.7), la Suisse devrait disposer des moyens juridiques lui permettant de traiter au besoin de manière diligente ces risques, quand bien même l'approche générale et non discriminante des risques sécuritaires doit continuer à être privilégiée tant que faire se peut (cf. ch. 4.1). Il convient dès lors de prévoir dans la LTC: une nouvelle disposition donnant au Conseil fédéral la possibilité de prendre les mesures qui s'imposent lorsqu'un risque géopolitique potentiel se matérialise, dans le respect des obligations internationales de la Suisse. Il s'agit en définitive de permettre à notre pays d'agir au besoin rapidement au travers du Conseil fédéral afin de sauvegarder ses intérêts et de préserver sa sécurité intérieure et extérieure, ainsi que son indépendance.

Le Conseil fédéral devrait ainsi se voir reconnaître dans la LTC la faculté de prendre par voie d'ordonnance les mesures potentielles de sauvegarde suivantes qui visent à renforcer la sécurité des infrastructures numériques et de télécommunication, dans la ligne de ce qui est envisagé par l'UE dans la boîte à outils 5G et par ses pays membres dans leur législation:

- Obliger les opérateurs de télécommunication à acquérir, mettre en place et exploiter des équipements, installations et logiciels liés à l'offre de services de télécommunication uniquement auprès de fournisseurs ou de catégories de fournisseurs d'équipements déterminés;
- Restreindre, suspendre ou interdire l'acquisition, la mise en place et l'exploitation d'équipements, d'installations et de logiciels liés à l'offre de services de télécommunications provenant de fournisseurs d'équipements qui sont jugés problématiques pour la sécurité de notre pays ou qui sont détenus, contrôlés ou sous l'influence d'un Etat étranger présentant un risque géopolitique pour la Suisse;
- Obliger les opérateurs à retirer de leur infrastructure les équipements, installations et logiciels liés à l'offre de services de télécommunication provenant de fournisseurs d'équipements qui sont jugés problématiques pour la sécurité de notre pays ou qui sont détenus, contrôlés ou sous l'influence d'un Etat étranger présentant un risque géopolitique pour la Suisse.

La prise des mesures envisagées ici pourrait avoir d'importantes conséquences économiques sur les opérateurs concernés, ainsi que des répercussions opérationnelles majeures sur leurs réseaux et sur leur offre de services de télécommunication. Elle devrait être envisagée avec prudence dans le respect des droits fondamentaux des entreprises concernées et soumise à des périodes de mise œuvre suffisamment longues.

4.3 Développer les capacités d'audit et de certification techniques

La sécurisation des infrastructures numériques, des équipements et installations de télécommunication et des produits TIC passe par leur certification ou évaluation de leur conformité en matière de sécurité (cf. ch. 3.2 et 3.4). Cela nécessite des compétences, des matériels et des expertises dont la Suisse dispose en fait largement au sein de ses hautes-écoles, de son secteur public ou de ses entreprises.

Les capacités d'audit et de certification sont en développement dans notre pays, comme le montre la création récente du NCSC qui dispose de compétences pointues en matière de cybersécurité ou l'essor exponentiel de l'offre privée de services d'analyses de vulnérabilité et de tests d'intrusion[20]. Le Cyber-Defence Campus (CYD Campus) d'armasuisse collabore par ailleurs étroitement avec les hautes écoles et les milieux économiques afin de mettre en place un monitorage des technologies axé sur la cybersécurité et les Académies suisses des sciences ont pour mandat d'évaluer les chances et risques des nouvelles technologies.

Cet écosystème suisse de la cybersécurité devrait être à même à terme de fournir à la Suisse les organismes nationaux de contrôle et de certification indépendants dont elle a besoin pour évaluer la sécurité tant logicielle que matérielle de ses infrastructures numériques, de ses équipements de télécommunication et de ses produits TIC. En parallèle, la Suisse devrait développer des accords internationaux de reconnaissance de certifications techniques, en particulier dans le cadre de l'accord de reconnaissance mutuelle Suisse – Union européenne (ARM CH-UE; RS 0.946.526.81).

4.4 Intensifier la coopération internationale

Une collaboration internationale est indispensable pour garantir la sécurité des réseaux et des infrastructures numériques compte tenu de leur interconnexion à l'échelle mondiale. Conformément à la stratégie de politique extérieure numérique 2021-2024[21], la Suisse veut renforcer la cybersécurité en défendant la mise en place concrète de normes de droit international[22]. Elle participe ainsi aux négociations en vue d'élaborer une convention des Nations Unies (NU) relative à la cybercriminalité, négocie la mise à jour de l'agenda mondial de la cybersécurité de l'Union internationale des télécommunications (UIT), participe activement à l'application des mesures de confiance dans le domaine de la cybersécurité de l'Organisation pour la sécurité et la coopération en Europe (OSCE) et soutien nombre d'initiatives internationales visant à maintenir un cyberespace ouvert, libre et sûr[23]. L'implication de la Suisse dans la réglementation internationale passe aussi par la «Genève internationale» qui constitue une plateforme essentielle des débats sur la cybersécurité à un niveau mondial.

Les États ne peuvent pas garantir à eux seuls la sécurité de l'espace numérique, dans la mesure où les acteurs de l'économie privée y jouent un rôle décisif avec leurs normes, leurs produits et leurs services globaux. C'est pourquoi la Suisse défend une approche multipartite et encourage le dialogue avec les entreprises. La collaboration avec des initiatives internationales privées et des centres de compétence techniques de cybersécurité (notamment FIRST, TF-CSIRT, NatCSIRT) revêt aussi une

---

[20] A l'exemple de l'Institut national de test pour la cybersécurité (NTC) basé à Zoug, qui vérifie la fiabilité et la sécurité des produits connectés et des applications numériques. Les tests sont lancés en coopération avec l'économie, les entreprises de sécurité informatique et les hautes écoles et s'appuient sur les normes internationales courantes. Le NTC a audité le certificat COVID-19 en juin 2021 et l'application chinoise «TikTok» en avril 2023 pour le compte du NCSC.

[21] Rapport du Conseil fédéral du 4 novembre 2020, Stratégie de politique extérieure numérique 2021–2024, en réponse au postulat 17.3789.

[22] Il convient à cet égard de mentionner l'engagement actif de la Suisse au sein de «Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security» (UN OEWG), mandaté par l'Assemblée générale de l'ONU.

[23] La Suisse sponsorise en particulier un programme des NU pour encourager un comportement responsable des États dans le cyberespace et s'engage dans la *Counter Ransomware Initiative*.

grande importance, ainsi que la participation à la normalisation des réseaux de télécommunication au sein de différentes organisations (UIT, ETSI, 3GPP, etc.) en collaboration avec les fournisseurs d'équipements.

5 Conclusion

Conformément à l'orientation stratégique de la législature 2023 à 2027, la Confédération doit anticiper les cyberrisques et prendre à cet égard des mesures efficaces visant à protéger la population, l'économie et les infrastructures critiques. La Stratégie nationale 2023 de protection des infrastructures critiques et la cyberstratégie nationale 2023 contre les cybermenaces reprennent cette approche préventive, tout en chargeant le Conseil fédéral d'analyser les risques et vulnérabilités cybers et de proposer les réglementations qui s'imposent compte tenu des besoins et lacunes légales.

Au vu des risques techniques à composante géopolitique que la Suisse court en lien avec ses infrastructures de télécommunication et numériques, le Conseil fédéral est convaincu qu'il y a lieu de renforcer les moyens de lutter contre ces risques et propose en conséquence des mesures à prendre sur la base de la LTC (stratégie «multi-fournisseurs», contraintes pour les équipements jugés à risque, exigences sécuritaires renforcées lors de la prochaine mise au concours de fréquences). Pour le reste, l'écosystème suisse de la cybersécurité devrait être à même à terme de fournir les organismes nationaux de contrôle et de certification dont notre pays a besoin.

A l'instar de ce qui est envisagé par l'UE dans la boîte à outils 5G et dans d'autres projets de réglementation notamment sur la cyber-résilience, le Conseil fédéral estime nécessaire de prévoir dans la LTC une nouvelle disposition qui lui donne la possibilité de prendre les mesures qui s'imposent lorsqu'un tel risque géopolitique se matérialise, ceci dans le respect des obligations internationales de la Suisse. Il s'agirait en particulier d'interdire si nécessaire l'acquisition, la mise en place et l'exploitation d'équipements provenant de fournisseurs jugés problématiques pour la sécurité de notre pays ou qui sont détenus, contrôlés ou sous l'influence d'un Etat étranger présentant un risque géopolitique pour la Suisse. A cet égard, la liberté économique et le bon fonctionnement de la concurrence doivent être garantis dans la mesure du possible.

Finalement, la Suisse doit continuer à s'engager dans une collaboration internationale qui est indispensable pour garantir la sécurité des réseaux et des infrastructures numériques compte tenu de leur interconnexion à l'échelle mondiale.