Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat

Berne, le [Datum]

« Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense »

Rapport du Conseil fédéral
En réponse aux postulats Dobler 19.3135 « Acquisitions de l'armée. Avons-nous la maîtrise de la cybersécurité ? » et 19.3136 « Infrastructures critiques. Avons-nous la maîtrise des composants matériels et logiciels ? » du 18 mars 2019

Table des matières

Sommaire

Au-delà des avantages notables qu'apporte l'utilisation des technologies de l'information et de la communication (TIC), elle s'accompagne également de risques considérables. Différentes mesures sont entreprises pour faire face à ces cyberrisques. Elles comprennent la prévention des défaillances et des manipulations, le renforcement de la résilience ou la mise en place de dispositifs de défense. Les efforts visant à atténuer les cyberrisques se butent au fait qu'il n'a pas encore été possible d'améliorer de manière adéquate la sécurité des produits TIC, qui présentent toujours de nombreuses failles de sécurité.

L'application de standards de sécurité peut pallier ce problème. Le rapport expose les standards existants dans le domaine de la sécurité des produits et de la gestion des risques de la chaîne d'approvisionnement, ainsi que les engagements qui en découlent pour la Confédération et les exploitants des infrastructures critiques. L'analyse montre qu'il existe de nombreux standards dans le domaine de la sécurité des produits et de leur utilisation sûre. L'application de certains de ces standards relatifs à la sécurité des produits est également très répandue. Les directives en matière de gestion des risques de la chaîne d'approvisionnement dans le domaine de la cybersécurité sont nettement moins développées.

Le rapport aborde ensuite le cadre juridique de l'application de ces standards dans l'administration fédérale et les infrastructures critiques. Il conclut que la base légale nécessaire à l'application systématique des standards de sécurité des produits TIC et de la gestion des risques de la chaîne d'approvisionnement pour la Confédération est en place, alors que les dispositions en rapport avec le respect des standards de sécurité des TIC pour les infrastructures critiques sont rares.

Enfin, le rapport indique dans quelle mesure les standards sont effectivement appliqués dans l'administration fédérale, l'armée et les infrastructures critiques. Les directives en matière de sécurité et d'utilisation sûre des produits TIC sont nombreuses au sein de l'administration fédérale et de l'armée. Le rapport conclut, en ce qui concerne les standards de sécurité des produits, que l'accent doit davantage être mis sur une mise en œuvre globale et continue des directives ainsi que sur le contrôle de celle-ci, plutôt que sur le développement de standards et de directives déjà largement établis. Les directives en matière de gestion des risques de la chaîne d'approvisionnement dans le domaine de la cybersécurité sont nettement moins développées. Il n'existe en outre aucune base légale qui impose la mise en œuvre d'une gestion des risques systématique. La majorité des standards mettant l'accent sur les processus et méthodes, ils tiennent plus d'instructions recommandées que de normes contraignantes.

En comparaison de la situation dans l'administration fédérale, peu de directives contraignantes pour la sécurité et l'utilisation sûre des produits TIC existent pour les infrastructures critiques. La création de nouvelles directives juridiquement contraignantes semble être la solution la plus évidente pour une meilleure diffusion des standards. Les références aux standards dans la domaine de la sécurité des produits représentent une autre possibilité. Des directives à l'attention des exploitants d'infrastructures critiques pour une gestion sûre des produits TIC seraient en outre envisageables. En principe, des directives relatives à des mesures régulatrices pour la gestion des risques de la chaîne d'approvisionnement pourraient également être introduites.

1 Introduction

La numérisation progresse à grande allure en Suisse. Aujourd'hui, toutes les autorités et entreprises sont connectées. Les technologies de l'information et de la communication (TIC) ont pris tellement d'ampleur que si celles-ci tombaient en panne ou cessaient de fonctionner correctement, la majorité des prestations de notre société ne pourraient être réalisées. Au-delà des avantages qu'apporte l'utilisation des TIC, elle s'accompagne de risques considérables appelés cyberrisques. Différentes mesures sont entreprises pour y faire face. Des mesures préventives organisationnelles et techniques visent à empêcher la manipulation et les défaillances des TIC. Des mesures de renforcement de la résilience doivent également permettre aux organisations de continuer à fonctionner même en cas de défaillance des TIC. De plus, des dispositifs de défense contre les attaques visant les TIC sont mis en place.

Ces efforts de réduction des cyberrisques se butent néanmoins au fait qu'il n'ait pas encore été possible d'améliorer de manière adéquate la sécurité des produits TIC. Ces produits présentent toujours de nombreuses failles de sécurité pour des raisons autant politiques qu'économiques. Ces dernières ont été soulignées par plusieurs chercheurs il y a déjà 20 ans[1]. Tout d'abord, le marché des produits TIC peut être qualifié d'économie en réseau. Les consommateurs n'achètent un produit que s'ils pensent que beaucoup d'autres consommateurs prennent la même décision. De cette façon, une collaboration entre partenaires permet d'éviter des coûts supplémentaires. C'est pourquoi il est essentiel pour les fabricants que leurs produits trouvent une large clientèle le plus vite possible et s'établissent comme la nouvelle solution par défaut. En conséquence, ils essaient de mettre leur produit sur le marché aussi tôt que possible et règlent les éventuels problèmes, comme les failles de sécurité, une fois que le produit s'est imposé[2]. Ensuite, l'asymétrie en matière d'information entre les prestataires et les acheteurs contribue au manque de sécurité des produits TIC. Les acheteurs ne pouvant évaluer la qualité des produits lors de l'achat, les prestataires n'ont aucun intérêt à la garantir quoi qu'il arrive. Le manque de transparence en matière de sécurité fait que les prestataires n'accordent pas la priorité à la sécurité de leurs produits[3].

Outre ces facteurs économiques, des facteurs géopolitiques gagnent en importance. Les marchés des produits TIC sont de plus en plus considérés comme un domaine d'intérêt sur le plan de la politique de sécurité. Le grand public, au moins depuis les révélations d'Edward Snowden en 2013, est parfaitement conscient que les gouvernements n'hésitent pas à influencer directement les fabricants de produits TIC pour accéder à leurs données. La confiance dans la sécurité des produits TIC s'en est trouvée davantage ébranlée, et de nombreux États ont constaté que la dépendance de leur économie et leur société aux TIC, qui sont produites en majorité dans des nations au statut de grandes puissances, pose un problème du point de vue de la politique de sécurité.

Ni les caractéristiques du marché des TIC ni la domination d'un petit nombre de fabricants provenant de grandes puissances ne vont changer à court et moyen terme, et les produits TIC ne seront jamais complètement sûrs. Il convient cependant d'examiner les possibilités d'améliorer la sécurité des produits TIC dans les domaines critiques pour la Suisse. L'application de normes de sécurité peut également jouer un rôle important. Il existe déjà à l'heure actuelle de nombreux standards de sécurité dont l'usage est répandu et qui sont constamment développés. En définissant des critères clairs et quantifiables pour la sécurité, ces standards améliorent la transparence et contribuent à faire de la sécurité un critère de qualité identifiable. Une demande systématique de la part des entreprises et des autorités quant à l'application de standards pourrait pousser les fabricants à mieux tenir compte de la sécurité.

Le présent rapport vise à montrer quelles mesures sont mises en place par la Confédération et notamment l'armée pour les acquisitions relatives à la sécurité, quelles mesures sont prises par les exploitants des infrastructures critiques et à quel niveau il pourrait être nécessaire d'intervenir.

---

[1] GORDON/LOEB: "The economics of information security investment", ACM Transactions on Privacy and Security Volume 5, Issue 4, 2002; ANDERSON/MOORE: "The economics of information security", Science, Vol. 314, 2006, pp. 610-613.

[2] SHAPIRO/VARIAN: "Information Rules. A Strategic Guide to the Network Economy", Boston, Harvard Business School Press, 1998.

[3] GEORGE A. AKERLOF: The market for 'lemons': Quality, uncertainty and the market mechanism. The Quarterly Journal of Economics, Vol. 84, 1970, pp. 488–500;
RAINER BÖHME: A Comparison of Market Approaches to Software Vulnerability disclosure, in: G. Müller (Ed): Emerging Trends in Information and Communication Security, ETRICS 2006, pp. 298-311; part of the Lecture Notes in Computer Science book series (LNCS, volume 3995), Springer, Berlin, Heidelberg

1.1 Contexte

La « Stratégie nationale de protection de la Suisse contre les cyberrisques 2018 – 2022 » (SNPC)[4] décrit les mesures de la Confédération, des cantons, des milieux économiques et des hautes écoles pour réduire les cyberrisques actuels. Elle définit des mesures de standardisation et d'encouragement de la résilience des infrastructures critiques face aux cyberrisques, sans toutefois aborder de manière explicite les risques de la chaîne d'approvisionnement. La nouvelle « Stratégie cyber du DDPS » de mars 2021, qui indique comment le DDPS s'investit dans la SNPC générale, établit un rapport direct avec la sécurité des chaînes d'approvisionnement et l'importance des standards internationaux[5].
La « Stratégie nationale de protection des infrastructures critiques 2018 - 2022 » (PIC)[6] aborde également les risques en lien avec les chaînes d'approvisionnement et l'importance des standards dans le cadre des mesures de vérification générale du respect des directives et d'encouragement de la résilience.
Les analyses et conclusions du présent rapport viennent compléter le contexte stratégique actuel. Elles visent à contribuer à la stratégie de gestion des risques en ce qui concerne la chaîne d'approvisionnement.

1.2 Mandat

Le présent rapport répond aux postulats Dobler 19.3135 et Dobler 19.3136 du 21 juin 2019. Ces postulats sont les suivants :

- **Postulat 19.3135 « Acquisitions de l'armée. Avons-nous la maîtrise de la cybersécurité ? »**
  La sécurité nationale repose notamment sur une armée suisse dotée de systèmes d'armes et d'une infrastructure en parfait état de fonctionnement. L'armée achète des systèmes d'armes et des systèmes d'infrastructure auprès de différents fournisseurs nationaux ou internationaux. Or, la disponibilité, la confidentialité et l'intégrité physique des composants cyberphysiques[7] de ces systèmes tendent à devenir le maillon faible de la capacité d'agir durablement et de la disponibilité opérationnelle des troupes terrestres et des forces aériennes suisses. Plus particulièrement, l'intégrité des acquisitions numériques (accès non documentés, vulnérabilités implantées intentionnellement) se révèle préoccupante.
  Le Conseil fédéral est chargé d'analyser les standards nationaux et internationaux (par ex. référentiel cybersécurité du NIST américain [National Institute of Standards and Technology], normes ISO, critères communs, NIST 800-161, EU4, EU5, FIPS) applicables à la gestion des risques du fournisseur et à la sécurité des composants cyberphysiques de l'armée, surtout des composants interconnectés, et de rendre ses conclusions sous la forme d'un rapport. Ce rapport s'intéressera notamment au contrôle de sécurité dont font l'objet les acquisitions. Il s'agit de vérifier si les directives actuelles (y compris de l'OMC) sont suffisantes pour répondre aux besoins de sécurité accrus liés aux nouvelles cybermenaces. Il se posera enfin dans ce contexte la question de savoir si dans les circonstances actuelles (du fait par ex. de produits achetés auprès de fournisseurs étrangers qui n'ont pas communiqué leur code source) l'armée suisse, avec ses partenaires en matière de sécurité, est même simplement en mesure de sauvegarder la souveraineté de la Suisse.

[4] Le Conseil fédéral suisse, Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018 – 2022 du 18 avril 2018, https://www.ncsc.admin.ch/dam/ncsc/fr/dokumente/strategie/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_FR.pdf
[5] Département de la défense, de la protection de la population et des sports, La Stratégie cyber du DDPS ; mars 2021, https://www.newsd.admin.ch/newsd/message/attachments/66203.pdf
[6] Le Conseil fédéral suisse, Stratégie nationale pour la protection des infrastructures critiques 2018–2022 du 8 décembre 2017 (PIC, FF 2018 491), https://www.babs.admin.ch/content/babs-internet/fr/aufgabenbabs/ski/_jcr_content/contentPar/tabs/items/downloads/tabPar/downloadlist/downloadItems/67_1460980334945.download/natstratski2018-2022_fr.pdf
[7] Le terme « cyberphysique » désigne l'association du monde numérique et du monde physique. Dans un système cyberphysique, les composants mécaniques sont reliés entre eux via des réseaux et des technologies de l'information de pointe.

Une fois que le Conseil fédéral sera en possession de ces informations, il voudra bien indiquer si les mesures actuelles suffisent à ses yeux pour identifier les risques, les évaluer et les ramener à un niveau acceptable.

- **Postulat 19.3136 « Infrastructures critiques. Avons-nous la maîtrise des composants matériels et logiciels ? »**
  La sécurité et l'approvisionnement de la Suisse reposent notamment sur des infrastructures critiques en parfait état de fonctionnement. Les exploitants de ces infrastructures achètent des systèmes et des composants informatiques auprès de différents fournisseurs nationaux ou internationaux.
  La complexité qui en résulte se traduit par des cyberrisques qui compromettent la disponibilité, la confidentialité et l'intégrité physique des infrastructures critiques et de la sécurité de l'approvisionnement du pays. Plus particulièrement, l'intégrité des acquisitions numériques (accès non signalés, vulnérabilités implantées intentionnellement) se révèle préoccupante.
  Le Conseil fédéral est chargé d'analyser les standards nationaux et internationaux (par ex. référentiel cybersécurité du NIST américain, National Institute of Standards and Technology, normes ISO, critères communs, NIST 800-161, EU4, EU5, FIPS) applicables à la gestion des risques du fournisseur et à la sécurité des systèmes, surtout des systèmes interconnectés, et de rendre ses conclusions sous la forme d'un rapport. Ce rapport s'intéressera également à la validité des standards, à leur mise en application actuelle et à leur respect pour l'ensemble des aspects touchant aux infrastructures critiques du pays et aux équipements nécessaires à leur bon fonctionnement.
  Une fois que le Conseil fédéral sera en possession de ces informations, il voudra bien indiquer si les mesures actuelles suffisent à ses yeux pour détecter les risques, les évaluer et les ramener à un niveau acceptable.

Outre la réponse à ces deux postulats, le rapport porte sur les demandes du document de réflexion « Supply Chain Security »[8] de septembre 2019 de la Commission Cybersécurité d'ICTswitzerland[9]. Les demandes qui y sont formulées concernant des conditions contractuelles spécifiquement axées sur la problématique de la chaîne d'approvisionnement, des exigences minimales en matière de sécurité des produits et un centre de contrôle pour la cybersécurité sont brièvement abordées dans le dernier chapitre au titre de mesures envisageables pour atténuer les risques au niveau des chaînes d'approvisionnement numériques.

Après une entrée en matière, le rapport aborde dans le chapitre 2 les principaux standards des domaines de la sécurité des produits pour les produits TIC et leur gestion des risques de la chaîne d'approvisionnement (*supply chain risk management*, SCRM). Le chapitre 3 traite des bases légales existantes pour l'application de ces standards en Suisse, et établit une distinction entre les bases pour la Confédération, les cantons et les communes et les bases pour les exploitants d'infrastructures critiques organisés selon le droit privé. Le chapitre 4 décrit où et comment les standards sont concrètement appliqués. Enfin, le chapitre 5 récapitule les conclusions, aborde les mesures possibles pour améliorer l'application des standards de sécurité des produits et de la SCRM des produits TIC et donne un aperçu des prochaines étapes.

1.3 Terminologie

Pour une meilleure compréhension du rapport, les termes principaux sont définis ci-après.

[8] ICTswitzerland : Supply Chain Security, Analyse et mesures visant à sécuriser la chaîne d'approvisionnement numérique, Groupe de travail Supply Chain Security de la Commission Cybersécurité d'ICTswitzerland, septembre 2019, https://digitalswitzerland.com/wp-content/uploads/2019/09/White_Paper_Supply_Chain_Security_2019_09_25_FR.pdf
[9] La faîtière ICTswitzerland a fusionné avec Digitalswitzerland au 01.01.2021 sous le nom Digitalswitzerland. La Commission Cybersécurité est maintenue.

1.3.1 Normes et standards

Dans l'usage, une confusion entre ces deux termes s'est installée au fil du temps, raison pour laquelle ils sont souvent utilisés de manière interchangeable. Cela s'explique par le fait qu'en anglais, aucune distinction n'est faite entre *norm* et *standard*.
Pour éviter le problème lié à la confusion entre les deux termes, standard est utilisé comme terme général dans les domaines techniques et scientifiques[10]. Étant donné son utilisation prépondérante dans les standards TIC internationaux et dans la langue anglaise, le présent rapport utilise également et exclusivement le terme *standard*.

1.3.2 Infrastructures critiques (IC)

Le terme IC est décrit comme suit dans la stratégie PIC : par infrastructures critiques (IC), 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[11].
En Suisse, les IC comprennent les domaines/secteurs suivants : les autorités, l'énergie, le traitement des déchets, la finance, la santé, l'information et la communication, l'alimentation, la sécurité publique, les transports.

1.3.3 Cyberrisques, cybersécurité et cyberdéfense

Dans le présent rapport, les termes en rapport avec les cyberrisques sont utilisés conformément à la terminologie de l'ordonnance sur les cyberrisques de la Confédération[12]. Les termes et domaines qui y figurent sont :

- **Cyberrisque :** risque de survenance d'un événement (résultant du produit de la probabilité de survenance et de l'étendue des dommages) nuisant à la confidentialité, à l'intégrité, à la disponibilité ou à la traçabilité des données ou pouvant occasionner des dysfonctionnements.
- **Domaine de la cybersécurité :** ensemble des mesures visant à prévenir et à gérer les incidents et à améliorer la résilience face aux cyberrisques ainsi qu'à développer la coopération internationale à cet effet.
- **Domaine de la cyberdéfense :** ensemble des mesures prises par les services de renseignement et l'armée dans le but de protéger les systèmes critiques dont dépend la défense nationale, de se défendre contre les cyberattaques, de garantir la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace et de développer ses capacités et compétences afin qu'elle puisse apporter un appui subsidiaire aux autorités civiles ; ce domaine inclut également des mesures visant à identifier les menaces et les attaquants ainsi qu'à entraver et à bloquer les attaques.

1.3.4 Sécurité des produits

L'expression « sécurité des produits » est marquée par son utilisation pour des produits physiques. L'accent est mis sur la sécurité et la santé des utilisateurs ainsi que des tiers lorsqu'ils utilisent les produits. La loi fédérale sur la sécurité des produits (LSPro)[13] exige que les produits mis sur le marché remplissent des exigences essentielles en matière de santé et de sécurité. Sa concrétisation prend la forme d'un renvoi à des normes techniques. On part du principe que ces exigences sont remplies lorsque les produits répondent aux normes et standards techniques et/ou organisationnels élaborés par

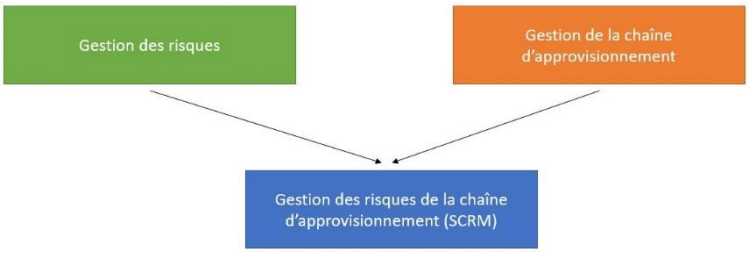
[10] Dans ce cas, un standard *de jure* correspondrait au terme norme. Pour faire la distinction avec le terme standard, le terme standard *de facto* est utilisé.
[11] Stratégie nationale pour la protection des infrastructures critiques 2018–2022 du 8 décembre 2017 (PIC, FF 2018 491)
[12] Ordonnance du 27 mai 2020 sur la protection contre les cyberrisques dans l'administration fédérale (Ordonnance sur les cyberrisques ; OPCy ; RS 120.73)
[13] Loi fédérale du 12 juin 2009 sur la sécurité des produits (LSPro ; RS 930.11)

des instances spécialisées (présomption de conformité)[14].

La sécurité des produits peut en revanche être décrite comme l'utilisation des produits TIC qui ne menace pas les objectifs de sécurité de la confidentialité, l'intégrité, la disponibilité ou la traçabilité des données. Il devient nettement plus difficile de déterminer comment développer une utilisation sûre des produits TIC à la différence de nombreux produits physiques. En conséquence, des directives relatives à leur utilisation doivent toujours être incluses lorsqu'il s'agit de leur sécurité. La sécurité des produits est employée dans le présent document comme une expression générique qui comprend à la fois la sécurité des produits TIC et leurs utilisation et intégration sûres au sein des infrastructures TIC.

1.3.5 Gestion des risques de la chaîne d'approvisionnement

La « gestion des risques du fournisseur » évoquée dans les postulats fait partie intégrante de la gestion des risques de la chaîne d'approvisionnement. Pour inscrire le rapport dans les discussions en cours concernant la SCRM dans le contexte de la cybersécurité, la notion plus large de « gestion des risques de la chaîne d'approvisionnement » (ou son abréviation SCRM) est utilisée à la place de « gestion des risques du fournisseur ». Sous cette notion figurent des concepts de gestion des entreprises et organisations développés sur de nombreuses années :



- **Gestion des risques :** désigne le processus systématique d'identification, d'analyse, d'évaluation et de gestion des risques[15].
- **Gestion de la chaîne d'approvisionnement :** désigne la mise en place et la gestion de chaînes logistiques intégrées (flux d'informations et de matériaux) sur l'ensemble du processus de création de valeur, de l'extraction des matières premières à l'utilisateur final en passant par les étapes de transformation[16].
- **Gestion des risques de la chaîne d'approvisionnement (SCRM) :** la SCRM associe la gestion des risques à la gestion de la chaîne d'approvisionnement. Les risques survenant le long de la chaîne d'approvisionnement doivent être identifiés, analysés, évalués et réduits[17].
  Des notions similaires et apparentées à SCRM sont :
  - Gestion des risques du fournisseur : partie de la SCRM qui porte sur l'évaluation des fournisseurs de produits TIC et de prestations.
  - Gestion des risques liés aux tiers : partie de la SCRM axée non seulement sur les fournisseurs de produits TIC et de prestations, mais aussi sur tous les tiers ayant des relations contractuelles avec l'organisation.

À ces risques liés aux fournisseurs s'ajoute également le fait que les prestataires sont souvent des entreprises étrangères internationales soumises au cadre juridique de leur pays d'origine. Compte tenu de l'intensification de la concurrence internationale en matière d'influence dans l'espace numérique ces dernières années, les risques d'une ingérence directe des États sur ces fournisseurs ont augmenté.

Enfin, il s'agit également de risques concernant la qualité et la disponibilité des prestations. Les prestataires ne sont pas tous en mesure d'assurer la maintenance de leurs prestations sur le long terme. Le risque que les petits prestataires ne puissent pas exécuter le mandat est particulièrement marqué. Il importe également de noter que les entreprises sont fortement dépendantes du savoir-faire de certains collaborateurs occupant des postes clés, ce qui contribue à l'augmentation du risque de défaillance

[14] Ce qui correspond à la législation européenne sur la sécurité des produits : le concept « New Approach » de 1985, modernisé et complété par le « New Legislative Framework » en 2008, forme le cadre de la réglementation européenne des produits. En l'occurrence, la législation de l'UE se limite à constater les exigences essentielles concernant un produit. La concrétisation passe par des normes harmonisées ou d'autres spécifications techniques (référence à des normes). La Suisse a largement adopté les directives « New Approach » de l'UE.
[15] ISO 31000:2018
[16] Gabler Wirtschaftslexikon
[17] NIST Special Publication Supply Chain Risk Management 800-161, p. 2

d'une prestation. Enfin, il est possible que les prestataires soient eux-mêmes victimes d'attaques visant l'intégrité de leurs prestations : une méthode intéressante pour les pirates qui souhaitent contaminer les systèmes de plusieurs entreprises en une seule attaque ciblée.

2 Standards de sécurité des produits et de la SCRM pour les produits TIC

Les standards, en permettant la compatibilité entre les appareils et en simplifiant grandement l'utilisation d'appareils de fabricants différents, ont toujours joué un rôle décisif dans l'informatique et la télécommunication. Un grand nombre de ces standards sont directement définis par les grands fabricants et imposés sur le marché. En parallèle, des processus de standardisation à proprement parler réunissent les fabricants, les utilisateurs, mais également les autorités et les organisations internationales en vue de s'accorder sur des standards. Ils représentent, dans le secteur dynamique et mondialisé des TIC, une tentative de s'accorder sur des règles dans des domaines présentant un intérêt commun marqué et une forte interdépendance. La sécurité des moyens TIC utilisés fait partie de ces domaines. Les appareils peu sûrs nuisent à la sécurité de tous les appareils connectés au réseau commun. Des standards ont par conséquent été développés très tôt pour évaluer la sécurité des moyens informatiques. En 1983 déjà, le gouvernement américain avait publié le standard TCSEC (*Trusted Computer System Evaluation Criteria*) qui est encore largement appliqué de nos jours via le standard « Critères communs ». Outre ces standards axés sur la sécurité des produits, de nombreux standards pour les procédures de sécurité liées aux TIC ont été et sont encore développés. Ceci car la majorité des problèmes de sécurité ne relèvent pas de déficiences des produits utilisés, mais plutôt d'une utilisation incorrecte ou d'une mise en œuvre lacunaire des mesures de protection.
Ces développements ont mené à la création d'un vaste éventail de standards pour la sécurité des produits TIC et des procédures associées. Il est cependant souvent compliqué pour les utilisateurs d'identifier les standards les plus adaptés et de prévoir les développements futurs en matière de standardisation. De plus, peu de standards ont pu s'imposer à l'échelle mondiale. C'est pourquoi le caractère quasi contraignant qui est espéré à travers une application exhaustive de standards de sécurité est rarement obtenu.

2.1 Caractère contraignant des standards

Les standards n'ont pas de valeur juridique à proprement parler, puisqu'ils sont établis par des organisations de droit privé qui ne sont pas autorisées à légiférer. L'application de standards est donc volontaire ou correspond à un besoin réel. Ils ne sont contraignants que lorsque leur respect est prescrit par la législation ou lorsqu'ils font l'objet d'un contrat entre plusieurs parties.
Les standards servent également à concrétiser des termes juridiques autrement imprécis, à l'instar de la formule *état de la technique*, et peuvent ainsi contribuer immédiatement à la sécurité juridique, malgré l'absence de caractère contraignant. Ils sont considérés dans de nombreux cas comme des règles de la technique claires et reconnues dont le respect constitue une étape importante dans la preuve d'une bonne conduite.

2.2 Standards de la sécurité des produits

Quelques-uns des standards les plus utilisés dans le domaine de la cybersécurité, accompagnés du nom de l'organisme de normalisation et d'une brève description de leurs particularités, sont énumérés dans la liste non exhaustive ci-dessous :

Désignation	**Application**
NIST Cybersecurity Framework *(National Institute of Standards and Technology, U.S. Department of Commerce)*	Standard de cybersécurité général qui couvre de manière générique tous types de cyberrisques.
Suite ISO/IEC 27000 *(Organisation internationale de normalisation / Commission électrotechnique internationale)*	L'organisation internationale de normalisation (ISO) publie différents standards pour la sécurité informatique qui se complètent, connus sous le nom « Suite 2700x ». Le standard ISO 27001 est le plus connu. Il définit les exigences pour la mise en place, la mise en œuvre, le maintien et l'amélioration continue d'un système de management de la sécurité de l'information (SMSI) en tenant compte du contexte d'une organisation.
COBIT *(ISACA ; Information Systems Audit and Control Association)*	COBIT (Control Objectives for Information and Related Technology) est un référentiel de bonnes pratiques reconnu au niveau international pour la gouvernance et la gestion des systèmes d'information des entreprises. COBIT a été publié par l'organisation à but non lucratif ISACA et développé par des experts pour satisfaire aux exigences d'experts en TIC et de chefs d'entreprise. Le référentiel combine la gouvernance d'entreprise et les techniques de gestion et propose des principes, des pratiques, des modèles et des outils d'analyse pour aider les utilisateurs à accroître considérablement la valeur de leurs systèmes TIC et la confiance en ces systèmes.
Critères communs (CC) *Common Criteria for Information Technology Security Evaluation* *(Common Criteria Implementation Board)*	Les Critères communs sont un standard international qui définit les critères généraux pour l'évaluation de la sécurité des technologies de l'information et avec lequel il est possible d'évaluer et de contrôler la sécurité des produits logiciels et matériels selon ces critères. Fruit d'une collaboration internationale, les CC unifient plusieurs anciens standards nationaux (CTCPE pour le Canada, ITSEC pour l'Europe, TCSEC pour les États-Unis) pour créer une base commune de l'évaluation de la sécurité des données. Avec l'adoption de la norme ISO/IEC 15408 en 1999, les CC ont été reconnus comme un standard international. Ils spécifient différentes exigences fonctionnelles de sécurité pour atteindre les objectifs de sécurité précédemment fixés. Ils définissent en même temps les exigences en matière de contrôle qui permettent d'établir la confiance dans la sécurité du produit. L'intégration de ces exigences dans des accords internationaux constitue un autre objectif de la certification CC. Elle évite ainsi la nécessité d'effectuer plusieurs certifications différentes des produits TIC en fonction du pays.

Standards BSI *(Office fédéral allemand de la sécurité des technologies et de l'information – BSI)*	Les standards BSI 200-1, 200-2 et 200-3 sont des éléments essentiels de la méthodologie du BSI pour une protection de base des TIC. Les standards BSI comprennent des mesures, des approches et des recommandations pour les procédures, méthodes et processus concernant les différents aspects de la sécurité de l'information dans les entreprises et les autorités. L'objectif de ces standards est l'introduction et la mise en œuvre progressives d'un SMSI pour une meilleure conception des processus opérationnels et la protection des données. Ils sont entièrement compatibles avec le standard ISO/IEC 27001 et tiennent compte des recommandations du standard ISO/IEC 27002. La terminologie se rapproche également de celle des standards ISO.
Federal Information Processing Standards (FIPS) *(National Institute of Standards and Technology, U.S. Department of Commerce)*	Les FIPS sont des standards minimaux publics développés par le gouvernement des États-Unis pour une application dans les systèmes informatiques des agences gouvernementales américaines non militaires et des mandataires du gouvernement. Ces standards minimaux couvrent les exigences de plusieurs domaines d'application. Ils sont utilisés tant que des standards industriels équivalents n'ont pas encore été développés. Les fabricants de TIC appliquent également les FIPS sur une base volontaire dans des contrats n'impliquant pas le gouvernement. Un grand nombre de spécifications FIPS s'appuient sur la modification de standards communément utilisés (par ex. ANSI, IEEE, ISO).
ENISA Guidelines *(European Union Agency for Cybersecurity (ENISA) ; auparavant : European Network and Information Security Agency)*	L'ENISA a publié un ensemble de directives dans le domaine de la sécurité de l'information et des réseaux : - National Cyber Security Strategy (NCSS) Good Practice Guide - Good Practice Guide on Incident Reporting - Technical Guideline on Security Measures
Norme minimale pour améliorer la résilience informatique (Norme minimale TIC) *(Office fédéral pour l'approvisionnement économique du pays, OFAE)*	Standard général de cybersécurité qui traite de tous les types de cyberrisques de manière générique (basé sur le NIST Cybersecurity Framework, voir ci-dessus).

2.3 Standards de la SCRM

Il existe nettement moins de standards relatifs à la cybersécurité dans le domaine de la SCRM. Quelques standards de sécurité des TIC mentionnent également l'importance de la SCRM, mais ne fournissent que peu d'indications concrètes. Des règles contraignantes de l'utilisation des standards ne sont donc formulées que pour certains aspects de la SCRM, à l'instar des contrôles et certifications obligatoires des produits au moment de l'acquisition[18].

[18] En Suisse, par exemple, la sécurité des données des compteurs intelligents doit être contrôlée en vertu de l'ordonnance sur l'approvisionnement en électricité (OApEl). Ils sont certifiés par l'Institut fédéral de métrologie.

Les standards suivants sont particulièrement importants en ce qui concerne la SCRM :

Désignation	**Emploi**
NIST Special Publication 800-161 « Supply Chain Risk Management Practices for Federal Information Systems and Organizations » *(National Institute of Standards and Technology, U.S. Department of Commerce)*	Développement et mise en œuvre de stratégies, mesures et contrôles en matière de gestion des risques de la chaîne d'approvisionnement. Cette publication propose aux agences fédérales un guide pour identifier, évaluer et réduire les risques de la chaîne d'approvisionnement des TIC à tous les niveaux de l'organisation.
ISO/IEC 27001 – Annexe A.15 : Relations avec les fournisseurs	L'annexe A.15.1 concerne la sécurité de l'information dans les relations avec les fournisseurs. L'objectif est de protéger les actifs de valeur de l'organisation accessibles ou influencés par les fournisseurs.
ISO/IEC 90003	ISO/IEC 90003 est une directive pour l'application d'ISO 9001 (exigences relatives au système de management de la qualité) dans le cadre de l'acquisition, du développement, du fonctionnement et de la maintenance du développement de logiciels entre le fournisseur, le mandataire et le client.
Standardized Information Gathering (Questionnaire) SIG *(The Santa Fe Group / Shared Assessments)*	Questionnaire standardisé pour évaluer la qualité de la relation avec les fournisseurs et les risques de livraison utilisé essentiellement dans les pays anglo-saxons. Le SIG est un recueil de questions sur la sécurité de l'information et la protection des données de tiers basé sur plusieurs dispositions et cadres de contrôle. Le SIG est publié par l'organisation à but non lucratif Shared Assessments. Celle-ci met à jour le questionnaire SIG chaque année en tenant compte des nouvelles exigences en matière de sécurité et de protection des données, des modifications des dispositions ainsi que des dernières tendances et des bonnes pratiques dans la gestion des risques pour les fournisseurs tiers.

De nombreux d'autres standards, guides et directives pour l'amélioration de la sécurité de l'information en général et convenant notamment pour l'amélioration de la gestion des fournisseurs existent en parallèle à ces standards les plus courants établis à l'international. On y compte par exemple les recommandations des organisations professionnelles ou les travaux de recherche des universités et des entreprises spécialisées dans la sécurité des TIC. Ces standards traitent entre autres de sujets tels que le chiffrement, les signatures numériques, les fonctions de hachage, l'authentification, les preuves de communication, les services d'horodatage, la protection incendie, la résistance à l'effraction, l'effacement sécurisé des supports de données, etc.

3 Cadre juridique pour l'application des standards

Le cadre juridique constitue la base sur laquelle les mesures d'amélioration de la sécurité des produits et les mesures de réduction des risques de la chaîne d'approvisionnement s'appuient. Il ne contient en règle générale aucune référence directe aux standards, mais forment la base de leur application.

L'État se divise en deux sphères juridiques tout à fait différentes lorsqu'il s'agit d'acquisitions. Pour remplir ses tâches publiques et légales, et dès qu'il n'est pas en mesure de les réaliser par ses propres moyens, il doit s'adresser régulièrement au secteur privé. Le droit des marchés publics décrit la procédure dans laquelle le processus de décision doit s'inscrire. Si cette décision est prise, en tenant compte des exigences, y c. les contraintes en matière de sécurité, le soumissionnaire adéquat est choisi dans le cadre de la procédure d'adjudication. Les prestations requises par l'État et leurs caractéristiques pour la réalisation des tâches sont décrites dans les documents d'appel d'offres. Il n'y a pas d'application directe des réglementations en vigueur. L'autorité doit plutôt s'assurer par le contrat que les réglementations sont respectées. Les violations de tels accords sont ainsi sanctionnées par le biais du droit privé, notamment par une réparation du préjudice. Ce point s'applique aussi bien à l'administration fédérale (et donc les acquisitions pour l'armée[19]) qu'aux infrastructures critiques relevant du droit public ou privé, pour autant qu'elles exercent leurs activités en Suisse dans l'un des secteurs visés à l'art. 4, al. 2, LMP. C'est pourquoi, dans le cas de l'octroi d'une prestation sur le marché, le contrat est l'élément principal pour la mise en œuvre des aspects concernant la sécurité, car il définit l'objet du contrat, c'est-à-dire la prestation à fournir. Le respect des standards internationaux ou des exigences visant à assurer un certain niveau de protection par l'intermédiaire de critères obligatoires (critères d'aptitude et spécification techniques) ou de critères évalués (critères d'adjudication) peut être défini dans l'appel d'offres, convenu dans le contrat et vérifié pendant la réalisation de la prestation. La relation entre le mandant/commanditaire/client/acheteur et le mandataire/fabricant/fournisseur figure au centre de l'intérêt dans le domaine de la SCRM. En règle générale, elle est également décrite et définie dans le contrat.

3.1 Cadre juridique pour l'application de standards dans l'administration fédérale

Les possibilités et les procédures d'application de standards de la sécurité des produits et de la SCRM sont définies dans plusieurs ordonnances et lois fédérales. Jusqu'à récemment, il n'existait pas de directive légale fédérale générale pour le domaine de la sécurité des produits TIC et des informations traitées par ces produits. La nouvelle loi sur la sécurité de l'information (LSI) comble cette lacune.

3.1.1 La loi sur la sécurité de l'information (LSI)[20]

Le 18 décembre 2020, le Parlement a adopté la loi fédérale sur la sécurité de l'information (LSI)[21]. La LSI réunit dans une seule loi les aspects réglementaires les plus importants concernant la cybersécurité et la sécurité de l'information. Elle comprend non seulement des règles pour la sécurité des produits, mais aussi pour la SCRM des produits TIC, notamment la gestion des risques, la classification des informations, la sécurité informatique, les contrôles de sécurité relatifs aux personnes, la protection physique, la protection lors d'acquisitions délicates par des procédures de sécurité de fonctionnement, mais également des règles pour le soutien des exploitants des infrastructures critiques par la Confédération dans le domaine de la sécurité de l'information. La LSI s'applique aux autorités et aux organisations de la Confédération (y c. l'armée) et définit les exigences minimales à remplir en matière de protection des informations et des infrastructures informatiques. Toutefois, cette loi s'applique également aux autorités cantonales et aux entreprises de droit privé qui soutiennent la Confédération dans l'exercice de ses fonctions et par conséquent traitent des informations classifiées de la Confédération ou ont accès à des ressources informatiques de la Confédération. Ainsi, la Confédération cherche à développer une collaboration étroite avec les cantons et le secteur privé pour faire face à la montée des cybermenaces.

[19] L'armée ne peut effectuer d'achats elle-même étant donné qu'elle ne fait pas partie de l'administration fédérale (en vertu de l'OLOGA), mais constitue une institution spéciale basée sur la loi sur l'armée. Une gestion autonome n'est possible que dans le cadre de l'ordonnance sur l'administration de l'armée (OAA ; RS 510.301).
[20] Loi fédérale sur la sécurité de l'information au sein de la Confédération (Loi sur la sécurité de l'information ; LSI ; FF 2020 9665)
[21] La LSI n'est pas encore en vigueur. Les ordonnances d'exécution spécifiques sont en cours d'élaboration.

La LSI repose sur des standards reconnus internationalement, notamment ISO/IEC 27001 et ISO/IEC 27002. Elle met l'accent sur les informations et les systèmes critiques, mais aussi la standardisation des mesures afin d'améliorer de manière continue et économique la sécurité de l'information dans la Confédération et d'atteindre un niveau de sécurité homogène entre les autorités fédérales et les autres services. La LSI ne définit pas de mesures détaillées, notamment en raison du développement rapide des technologies, mais pose en revanche une base légale formelle sur laquelle les autorités administratives peuvent s'appuyer pour créer des ordonnances ou directives relatives à la sécurité de l'information.
La décision de la Confédération de réunir les différents aspects de la sécurité de l'information au sein d'une loi démontre l'importance qu'elle attache à ce sujet.

3.1.2 Standards de sécurité des produits TIC

L'ordonnance sur les cyberrisques, l'ordonnance concernant la protection des informations, mais aussi la loi fédérale sur la protection des données et l'ordonnance sur la protection des données définissent les bases pour l'application de standards relatifs à la sécurité des produits (y c. les directives pour une utilisation sûre des produits) dans l'administration fédérale.

Ordonnance sur les cyberrisques (OPCy)[22] **:** l'OPCy définit les directives en matière de sécurité informatique et d'utilisation sûre des TIC dans l'administration fédérale. Elle règle les compétences du délégué à la cybersécurité pour édicter les directives en matière de sécurité informatique pour les unités administratives de l'administration fédérale (art. 11, al. 1, let. e). Il peut participer à l'élaboration de directives ou de projets informatiques de la cybersécurité (art. 11, al. 3). L'OPCy impose également la réalisation de procédures de sécurité graduelles (art. 14*b* ss ; voir chap. 4.1.1), qui peuvent être complétées et élargies par les directives en matière de sécurité informatique édictées par le délégué. Ces procédures de sécurité constituent la base pour une réalisation sûre de tous les processus opérationnels assistés par ordinateur et veillent à ce que les services concernés soient impliqués au moment opportun. Cela s'applique tout au long du cycle de vie des systèmes TIC, en d'autres termes, du début d'un nouveau projet jusqu'à son arrêt. On garantit ainsi que chaque partie assume correctement ses responsabilités au cours des différentes étapes.

Ordonnance concernant la protection des informations (OPrI)[23] **:** l'OPrI règle la protection des informations de la Confédération et de l'armée, dans la mesure où elle est nécessaire dans l'intérêt du pays. Elle fixe notamment la classification (art. 4 ss) et les formes de traitement des informations qui en découlent (art. 13 ss). Le Conseil fédéral a fixé dans l'annexe de l'OPrI des exigences techniques pour la sécurité des produits des systèmes TIC prévues pour le traitement des informations classifiées. L'entrée en vigueur de la LSI signifie l'abrogation de l'OPrI. Dans la mesure où les contenus nécessaires ne figurent pas déjà dans la loi, ils sont reportés dans une nouvelle ordonnance sur la sécurité de l'information.

Loi fédérale sur la protection des données et ordonnance relative à la loi fédérale sur la protection des données (LPD et OLPD)[24] **:** la loi fédérale sur la protection des données (LPD) et l'ordonnance correspondante définissent les exigences organisationnelles et techniques pour le traitement des données personnelles (art. 7, 11 et 17*a* LPD, art. 8-11, 20 et 21 OLPD). Elles définissent ainsi les standards minimaux pour la sécurité des produits TIC utilisés pour le traitement de ce type de données.

[22] Ordonnance sur la protection contre les cyberrisques dans l'administration fédérale (Ordonnance sur les cyberrisques ; OPCy ; RS 120.73)
[23] Ordonnance concernant la protection des informations de la Confédération (Ordonnance concernant la protection des informations, OPrI ; RS 510.411)
[24] Loi fédérale sur la protection des données (LPD ; RS 235.1) et ordonnance relative à la loi fédérale sur la protection des données (OLPD ; RS 235.11).

3.1.3 Standards pour la SCRM

Il convient d'abord d'identifier les possibilités juridiques dans la conception des processus d'achats pour appliquer des standards dans le domaine de la SCRM. Les bases nécessaires figurent dans le droit des marchés publics. En outre, des conditions importantes ont été créées dans l'ordonnance concernant la sauvegarde du secret et l'ordonnance sur les contrôles de sécurité relatifs aux personnes pour contrôler plus rigoureusement les prestataires de services et produits relatifs à la sécurité.

Droit des marchés publics –Accord dans le cadre de l'Organisation mondiale du commerce (OMC) et loi fédérale sur les marchés publics (LMP)[25] **:** en adhérant à l'Organisation mondiale du commerce (OMC), la Suisse s'est engagée à libéraliser le commerce international et à supprimer les éventuels obstacles au commerce dans son système juridique. Le droit international reconnaît cependant que les États peuvent avoir besoin de déroger au principe de libre-échange pour protéger leurs intérêts essentiels de sécurité. L'accord du 15 avril 1994 instituant l'Organisation mondiale du commerce[26] et l'accord révisé sur les marchés publics[27] prévoient tous deux que les États signataires peuvent prendre des dispositions nécessaires à la protection de leurs intérêts de sécurité. En outre, la transmission d'informations dont la divulgation serait à l'encontre des intérêts de sécurité peut être refusée. Cela concerne notamment les acquisitions d'armes, de munition, de matériel de guerre ainsi que les acquisitions nécessaires à la sécurité ou la défense nationale. En ce qui concerne les contrats relevant de la sécurité ou de la défense nationale, les parties contractuelles doivent renoncer à recourir aux principes du droit international des marchés publics et notamment à ceux du traitement national et de la non-discrimination[28].

Le législateur a fait usage de la réserve de l'accord révisé sur les marchés publics pour protéger les intérêts essentiels de la sécurité nationale. Ainsi, il a fixé dans l'art. 10, al. 4, let. a, LMP, que les adjudications dont l'exemption est jugée nécessaire pour la protection et le maintien de la sécurité extérieure ou intérieure ou de l'ordre public ne sont plus soumises à la loi sur les marchés publics. Cette exception peut être utilisée par tous les mandants soumis à la LMP et n'est pas restreinte à l'administration fédérale centrale, ceci toujours dans le cadre de leur pouvoir d'appréciation (voir ch. 3 plus haut). Néanmoins, cette dérogation aux principes du libre-échange ne peut être sollicitée que dans le cadre de cet accord. Le service d'achats doit pouvoir démontrer l'impossibilité de réduire les risques à un niveau acceptable à l'aide de mesures raisonnables et non discriminantes. C'est pourquoi les critères constitutionnels continuent de s'appliquer. Ces décisions doivent notamment être non arbitraires et justifiées.

Ordonnance concernant la sauvegarde du secret[29] **:** l'ordonnance du 29 août 1990 concernant la sauvegarde du secret fixe les mesures de sécurité qui interviennent dans l'exécution d'un mandat par un tiers lorsque celui-ci contient des informations militaires classifiées de niveau CONFIDENTIEL et SECRET. Elle constitue la base légale pour réaliser les procédures d'habilitation de sécurité pour les mandataires de la Confédération ainsi qu'un élément central de la SCRM. La procédure d'habilitation de sécurité est désormais fondée sur une base légale formelle dans la LSI.

Ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP)[30] **:** l'ordonnance du 4 mars 2011 sur les contrôles de sécurité relatifs aux personnes règle, sur la base des art. 19-21 de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)[31] et des art. 23, al. 2, let. d, 103, al. 3, let. d, et 113, al. 4, let. d, de la loi fédérale sur l'armée et l'administration militaire (LAAM)[32], la condition pour l'exécution de contrôles de sécurité relatifs aux personnes. Cette base joue un rôle central en matière de gestion des risques liés aux collaborateurs des fournisseurs tiers. L'entrée en vigueur de la LSI permet à cette ordonnance de s'appuyer sur une nouvelle

[25] Loi fédérale sur les marchés publics (LMP ; RS 172.056.1)
[26] Accord instituant l'Organisation mondiale du commerce (RS 0.632.20)
[27] Accord révisé sur les marchés publics (RS 0.632.231.422)
[28] Cf. art. III de l'accord révisé sur les marchés publics (RS 0.632.231.422)
[29] Ordonnance concernant la procédure à suivre lors de la passation de contrats dont le contenu est classifié du point de vue militaire (Ordonnance concernant la sauvegarde du secret ; RS 510.413)
[30] Ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP ; RS 120.4)
[31] Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI ; RS 120)
[32] Loi fédérale sur l'armée et l'administration militaire (Loi sur l'armée ; LAAM ; RS 510.10)

base légale formelle et d'être totalement révisée.

3.2 Cadre juridique pour l'application de standards dans les infrastructures critiques

Il n'existe pas de loi en Suisse qui fixe des directives pour la sécurité ou l'acquisition de moyens TIC dans l'ensemble des secteurs des infrastructures critiques[33]. De telles directives, si elles existent, sont principalement faites dans des actes spécifiques au secteur. Ces actes s'inscrivant dans leurs contextes réglementaires respectifs, ils diffèrent grandement en ce qui concerne les directives pour la sécurité. On constate qu'en règle générale, peu de directives contraignantes relatives à l'application de standards de la sécurité des produits ou la SCRM sont édictées à l'attention des exploitants d'infrastructures critiques. Certains actes renvoient indirectement à des standards en demandant aux exploitants d'infrastructures critiques de prendre des mesures de sécurité correspondant à « l'état de la technique »[34]. Ces références indirectes concernant la sécurité des TIC sont relativement difficiles à interpréter, l'état actuel de la technique étant difficile à déterminer. Reste à savoir dans quelle mesure les standards internationaux doivent être appliqués pour remplir ce critère.
Le tableau suivant énumère les bases légales qui proposent des directives explicites en ce qui concerne la sécurité. Il montre en outre à partir de laquelle de ces bases se dégage une application obligatoire de standards pour une utilisation sûre des produits TIC et de leurs acquisitions.

Secteurs	Directive
Autorités et sécurité publique	Les bases légales mentionnées dans le chapitre 3.1 s'appliquent à l'administration fédérale.
Énergie	• L'ordonnance sur l'approvisionnement en électricité[35] (art. 8*b*) définit une vérification des systèmes de mesure intelligents effectuée par l'Institut fédéral de métrologie en ce qui concerne la sécurité de leurs données. La loi sur l'approvisionnement en électricité[36] (art. 20*a*) demande un contrôle de sécurité relatif aux personnes périodique pour les collaborateurs et les personnes mandatées de la société de gestionnaires du réseau nationale qui peuvent influer sur la sécurité du réseau de transport. • L'ordonnance sur le courant fort[37] (art. 4) et l'ordonnance sur le courant faible[38] (art. 4) font directement référence aux normes suisses et internationales applicables pour la sécurité des installations et les déclarent contraignantes. • La loi sur l'énergie nucléaire[39] et l'ordonnance sur l'énergie nucléaire[40] comprennent diverses prescriptions pour la sécurité de l'exploitation des installations nucléaires. L'ordonnance sur les contrôles de sécurité relatifs aux personnes dans le domaine des installations nucléaires[41] prévoit que toute personne ayant accès à des informations classifiées concernant des systèmes de sûreté ou de sécurité relatifs à des installations ou des matières nucléaires soit soumise à un contrôle de sécurité (art. 1).

[33] La nouvelle loi sur la sécurité de l'information (cf. chapitre 3.1) comprend des règlements qui s'appliquent également aux exploitants d'infrastructures critiques.
[34] Par ex. art. 3 de l'ordonnance sur la protection contre les accidents majeurs (Ordonnance sur les accidents majeurs ; OPAM ; RS 814.012) ; art. 3 de la loi fédérale sur la sécurité des produits (LSPro ; RS 930.11). La discussion porte surtout sur la référence à l'état de la technique en lien avec le règlement général sur la protection des données (RGPD) dans l'Union Européenne (UE).
[35] Ordonnance sur l'approvisionnement en électricité (OApEl ; RS 734.71)
[36] Loi sur l'approvisionnement en électricité (LApEl ; RS 734.7)
[37] Ordonnance sur les installations électriques à courant fort (Ordonnance sur le courant fort ; RS 734.2)
[38] Ordonnance sur les installations électriques à courant faible (Ordonnance sur le courant faible ; RS 734.1)
[39] Loi sur l'énergie nucléaire (LENu ; RS 732.1)
[40] Ordonnance sur l'énergie nucléaire (OENu ; RS 732.11)
[41] Ordonnance sur les contrôles de sécurité relatifs aux personnes dans le domaine des installations nucléaires (OCSPN ; RS 732.143.3)

	• Selon la loi sur les ouvrages d'accumulation[42] (art. 2), lesdits ouvrages doivent être dimensionnés, construits et exploités de sorte que leur sécurité reste assurée dans tous les cas de charge et d'exploitation prévisibles.
Traitement des déchets	• L'ordonnance sur les accidents majeurs[43] (art. 3) prescrit à certaines entreprises de prendre les mesures de sécurité correspondant à l'état de la technique qui tiennent compte des accidents majeurs propres à l'entreprise ou à son voisinage, comme des interventions de personnes non autorisées. L'ordonnance ne fait cependant aucune référence explicite à la sécurité des TIC et aux standards correspondants.
Finances	• La loi sur l'Autorité fédérale de surveillance des marchés financiers[44] confère à l'Autorité fédérale de surveillance des marchés financiers (FINMA) la compétence d'édicter les dispositions d'exécution concernant la protection et la sécurité des données (art. 13*a*, al. 3). L'ordonnance relative à la loi sur la surveillance des marchés financiers[45] fixe dans quelle mesure la FINMA fait usage de cette compétence et son obligation de tenir compte des standards internationaux (art. 5 et art. 6). • Les circulaires FINMA[46] 2017/01 Gouvernance d'entreprise – banques[47], 2008/7 Outsourcing – banques[48] et 2008/21 Risques opérationnels – banques[49] obligent les banques à mettre en œuvre des standards correspondant aux directives des standards NIST.
Santé	• L'ordonnance sur le dossier électronique du patient (ODEP)[50] prévoit que les communautés se dotent d'un système de gestion de la protection et de la sécurité des données (art. 12). L'ODEP fait ensuite référence à la norme ISO/IEC 29115:2013 (art. 23) en ce qui concerne la sécurité des moyens d'identification. En outre, l'accréditation de l'organisme de certification (art. 28) ainsi que les critères et les procédures de certification (art. 30-38) sont réglés.
Information et communication	• La loi sur les télécommunications (LTC)[51] (art. 48*a*) donne au Conseil fédéral la compétence d'édicter des prescriptions techniques et administratives pour assurer la sécurité des infrastructures de télécommunication.
Alimentation	• Aucune exigence de sécurité relative à l'informatique ou aux fournisseurs n'a été trouvée dans les ordonnances.
Transports	• Aucune exigence de sécurité relative à l'informatique ou aux fournisseurs n'a été trouvée dans les ordonnances. • L'ordonnance sur les accidents majeurs traite partiellement des voies de communication.

4 Application des standards

Les standards existants couvrant largement les mesures organisationnelles et techniques de cybersécurité, leur application permet de mettre en place une grande partie des mesures organisationnelles et techniques de protection contre les cyberrisques. Ce chapitre présente les mesures les plus importantes

[42] Loi fédérale sur les ouvrages d'accumulation (LOA ; RS 721.101)
[43] Ordonnance sur la protection contre les accidents majeurs (Ordonnance sur les accidents majeurs, OPAM ; RS 814.012)
[44] Loi sur l'Autorité fédérale de surveillance des marchés financiers (Loi sur la surveillance des marchés financiers, LFINMA ; RS 956.1)
[45] Ordonnance relative à la loi sur la surveillance des marchés financiers (RS 956.11)
[46] La FINMA explique dans ses circulaires la manière dont elle applique la législation sur les marchés financiers dans sa pratique de la surveillance. Les circulaires sont disponibles sous : https://finma.ch/fr/documentation/circulaires/
[47] Disponible sous : https://finma.ch/fr/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2017-01-20200101.pdf?la=fr
[48] Disponible sous : https://finma.ch/fr/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2008-07.pdf?la=fr
[49] Disponible sous : https://finma.ch/fr/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2008-21-20200101.pdf?la=fr
[50] Ordonnance sur le dossier électronique du patient (ODEP ; RS 816.11)
[51] Loi sur les télécommunications (LTC ; RS 784.10)

de l'administration fédérale et des exploitants d'infrastructures critiques qui représentent une application directe des directives des standards de la sécurité des produits et de la SCRM des produits TIC.

4.1 Application de standards dans l'administration fédérale

La sécurité des produits TIC est une priorité absolue de l'administration fédérale et de l'armée. Les directives existantes en matière de sécurité des produits et de SCRM sont adaptées au fur et à mesure. Elles s'inspirent fortement des standards internationaux en vigueur, mais en ne faisant qu'exceptionnellement de référence directe aux standards en question[52].

4.1.1 Application de standards de sécurité des produits TIC

En ce qui concerne les directives en vigueur, la mise en œuvre des mesures les plus importantes de sécurité des TIC au long de l'ensemble du cycle de vie d'un système TIC (planification, acquisition, exploitation, arrêt) est d'une importance vitale pour la qualité de la cybersécurité. C'est pourquoi chaque année, le Centre national pour la cybersécurité (NCSC) contrôle l'état de la mise en œuvre de ces mesures au sein de l'administration fédérale et en informe le Conseil fédéral. Un résumé de ces enquêtes est disponible[53]. Nous présentons ci-après le rôle que les standards de sécurité des produits TIC ont joué dans la mise en œuvre de ces mesures.

Les procédures de sécurité de l'administration fédérale

Les procédures de sécurité définies dans l'OPCy se composent des éléments suivants :

- Analyse des besoins de protection : tout projet informatique doit au préalable faire l'objet d'une analyse des besoins de protection. L'analyse des besoins de protection fournit une appréciation de l'évaluation de l'application ou du projet. Tout objet informatique doit disposer d'une analyse des besoins de protection récente. Une partie de l'analyse des besoins de protection est également le processus de réduction du risque d'espionnage par des services de renseignement (GRAES). Ce processus de contrôle a été élaboré dans le but d'identifier le besoin de protection de la fourniture d'une prestation informatique en prenant en compte la menace d'instrumentalisation de fournisseurs informatiques, de prendre les éventuelles mesures de protection et de les coordonner avec une possible procédure d'adjudication. Par la suite, les risques sont identifiés et les mesures qui doivent être incorporées dans le Concept de sécurité de l'information et de protection des données (concept SIPD) sont prises.
- Directives pour la protection de base : la « protection informatique de base dans l'administration fédérale » définit de manière contraignante les directives de sécurité minimales (protection de base) sur les plans de l'organisation, du personnel et de la technique en matière de sécurité informatique. La protection informatique de base doit au minimum être mise en œuvre pour chaque objet informatique à protéger. La mise en œuvre doit être documentée et contrôlée régulièrement par les unités administratives concernées.
- Directives de protection élevée : si l'analyse révèle des besoins de protection accrus, les unités administratives définissent, en plus de la mise en œuvre des directives en matière de sécurité relevant de la protection de base, d'autres mesures de sécurité sur la base d'une analyse des risques, documentent ces mesures et les mettent en œuvre. Le concept SIPD décrit les mesures de sécurité applicables à un objet informatique à protéger, leur mise en œuvre et les risques résiduels.

La Confédération met également en œuvre les mesures de protection suivantes :

[52] Les directives du 16 décembre 2016 sur la sécurité de l'information du DDPS (DSI DDPS) ainsi que les directives du 26 avril 2017 des responsables de la sécurité de l'information du DDPS contiennent des règles contraignantes pour le SMSI au niveau du DDPS ainsi que le SMSI des groupes et des offices du DDPS. Il est explicitement stipulé que le SMSI du DDPS est basé sur le standard SN ISO/IEC 27001:2015.
[53] https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/berichte/informatiksicherheitsberichte-bund.html

- Contrôle des produits cryptographiques : les produits cryptographiques[54] servent protéger les informations en termes de confidentialité, d'intégrité, d'authenticité ou d'obligation. L'acquisition et l'exploitation de ce type de produits sont particulièrement délicates, car le bon fonctionnement des fonctions cryptographiques ne peut être évalué et contrôlé que par des experts qualifiés. L'absence de contrôle et de vérification entraîne le risque que les produits cryptographiques ne puissent fonctionner comme prévu, sans que cela soit effectivement remarqué. C'est pour cela que les produits du domaine de la cryptologie sont achetés essentiellement par l'Office fédéral de l'armement (armasuisse) en tant qu'organisme spécialisé[55]. armasuisse est soutenu dans cette entreprise par le service de cryptologie de la Base d'aide au commandement de l'armée (BAC crypt). Ses experts effectuent des contrôles cryptologiques approfondis, que ce soit pendant l'acquisition ou pendant les changements de systèmes (par ex. après les mises à jour du firmware ou du logiciel) tout au long du cycle de vie du système.

- Analyse des vulnérabilités par le NCSC : le NCSC est le service de notification principal des vulnérabilités des applications de l'administration fédérale. Il effectue un contrôle de plausibilité des notifications reçues, une évaluation des risques que pose la vulnérabilité et prend les mesures adéquates après concertation avec les prestataires et les unités administratives concernés. Au DDPS, les spécialistes du Cyber Defence Campus sont constamment à la recherche de vulnérabilités et de points d'entrée dans les logiciels des systèmes et des applications du département.

- Système de management de la sécurité de l'information (SMSI) au DDPS : un SMSi définit les règles et méthodes pour assurer la sécurité de l'information dans une entreprise ou organisation. Sa fonction est d'identifier et de gérer les risques pour la sécurité de l'information et la cybersécurité (informations, données et informatique) en accord avec les objectifs organisationnels généraux. Le SMSI mis en place au DDPS s'appuie sur la norme ISO/IEC 27001.

4.1.2 Application de standards de la SCRM

Mesures relevant du droit des marchés publics : conformément à l'art. 20, al. 3, LMP, la procédure d'invitation peut être utilisée par le service demandeur pour l'acquisition d'armes, de munitions, de matériel de guerre ou, s'ils sont indispensables à des fins de défense et de sécurité, d'autres fournitures, de travaux de construction, de services, de travaux de recherche ou de développement. Dans ce cas, le service d'achats responsable définit quels prestataires il souhaite inviter à présenter une offre directement, sans passer par un appel d'offres public. Le droit des marchés publics autorise en conséquence une marge de manœuvre pour l'application de standards de la SCRM dans les acquisitions de services informatiques sensibles. Le choix en termes des prestataires de produits TIC liés à la sécurité pour les acquisitions relatives à la sécurité et la défense, et donc pour l'armée, peut être restreint d'après la LMP, en raison de leur nationalité par exemple.

Conclusion d'accords relatifs à la protection des informations : la Suisse dépend d'une collaboration étroite avec des partenaires internationaux et leurs bases industrielles pour assurer sa défense ainsi que pour la sécurité intérieure et extérieure. Les mandats attribués dans ces domaines sont souvent sensibles, c'est pourquoi la Suisse a conclu des accords relatifs à la protection des informations[56] avec de nombreux États et organisations internationales. Ils règlent la protection mutuelle des informations classifiées et fixent les mesures de sécurité pour les acquisitions bilatérales relatives à la sécurité.

[54] Exemples : appareil de chiffrement, Smartcard, Hardware Security Module (module de sécurité matériel), générateur de nombre aléatoire, logiciel de chiffrement, bibliothèque crypto, etc.
[55] Cf. art. 10, al. 1, let. d, de l'ordonnance sur l'organisation des marchés publics de l'administration fédérale (Org-OMP ; RS 172.056.15)
[56] Voir p. ex. l'accord entre le Conseil fédéral suisse et le Gouvernement de la République française relatif à l'échange et la protection réciproque des informations classifiées (RS 0.514.134.91) ou l'accord entre le Département fédéral de la défense, de la protection de la population et des sports, au nom du Conseil fédéral suisse et le Ministère fédéral de la Défense nationale de la République d'Autriche concernant la protection des informations militaires classifiées (RS 0.514.116.31).

Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense

La conclusion d'accords relatifs à la protection des informations implique que les parties contractuelles disposent d'instruments de sécurité dans leur droit national qui satisfont les standards reconnus internationalement. Concrètement, les accords relatifs à la protection des informations exigent que les entreprises et les personnes qui doivent exécuter des mandats classifiés pour l'autre partie fassent l'objet d'une procédure de certification de leur fiabilité.

Le standard international pour l'évaluation de la fiabilité des entreprises[57] exige entre autres de vérifier si l'entreprise est contrôlée ou influencée par des États ou des organisations étrangers de droit privé ou public (Foreign Ownership, Control and Influence – FOCI). Si le risque est trop important, il est nécessaire de prendre des mesures visant à le réduire ou d'exclure l'entreprise de la procédure d'adjudication. Cela vaut également pour les personnes physiques.

Les accords relatifs à la protection des informations ne fixent généralement pas d'exigences en matière de sécurité des produits. Cependant, ils stipulent souvent que les systèmes informatiques destinés à traiter les informations des autres parties sont accrédités par une autorité de sécurité nationale compétente. L'accréditation prouve que le système remplit les exigences en matière de sécurité de l'autre partie, constituant ainsi une confirmation formelle de la correspondance à la sécurité des produits.

Mise en œuvre des procédures de sauvegarde du secret : la procédure de sauvegarde du secret permet au mandant d'imposer des mesures de sécurité régaliennes au mandataire[58]. Cependant, cette procédure ne s'applique que lorsque des informations classifiées CONFIDENTIEL ou SECRET doivent être traitées. La première étape de la procédure de sauvegarde du secret consiste à contrôler, en coopération avec le Service de renseignement de la confédération (SRC), la fiabilité de l'entreprise concernée par le mandat. Un service spécialisé définit ensuite dans un protocole de sécurité officiel les mesures concrètes que l'entreprise doit suivre pendant l'exécution du mandat. Une fois toutes les mesures mises en œuvre, l'entreprise obtient une déclaration de sécurité d'entreprise. C'est un certificat reconnu internationalement qui habilite l'entreprise à exécuter le mandat classifié. Le service spécialisé peut inspecter à tout moment et sans prévis une entreprise au bénéfice d'une déclaration de sécurité relative aux entreprises pour contrôler le respect des exigences en matière de sécurité.
Les mandants sont en principe les unités administratives du DDPS et de l'Office fédéral des constructions et de la logistique (OFCL)[59]. Les mandataires sont des organismes publics extérieurs au DDPS et à l'OFCL, des entreprises privées ou des particuliers destinés à recevoir et à traiter des informations classifiées. Si le mandataire est une entreprise ayant son siège dans un pays tiers, le traitement des contrats sur le plan de la sécurité et les modalités de la collaboration entre les autorités de sécurité nationales respectives sont réglés dans le cadre de l'accord relatif à la protection des informations correspondant (voir ci-dessus). L'entreprise est alors contrôlée par les organes de sécurité du pays tiers. La LSI renomme la « procédure de sauvegarde du secret » en « procédure de sécurité relative aux entreprises » et étend celle-ci aux entreprises qui doivent exploiter, gérer, entretenir ou contrôler des systèmes d'information critiques de la Confédération (ou certaines parties de ces systèmes) dans le cadre d'un contrat.

Mise en œuvre des contrôles de sécurité relatifs aux personnes : si les personnes qui fournissent des prestations TIC ou développent des produits TIC ont accès à des informations classifiées CONFIDENTIEL ou SECRET, elles doivent être soumises à un contrôle de sécurité. Cela s'applique également au personnel des fournisseurs et des prestataires. Les organismes examinateurs peuvent ainsi avoir accès au casier judiciaire, à l'index national de police et au système informatique de la sécurité intérieure du SRC. Par la suite, les organismes examinateurs rendent une décision indiquant si la personne contrôlée est considérée comme sans danger ou comme un risque pour la sécurité. Cependant, cela ne

[57] Les standards du domaine de la sécurité industrielle internationale sont élaborés par le Multinational industrial security working group (MISWG). Ils ne sont pas contraignants, mais forment la base de la reconnaissance de l'équivalence de mesures.
[58] Voir l'ordonnance concernant la procédure à suivre lors de la passation de contrats dont le contenu est classifié du point de vue militaire (Ordonnance concernant la sauvegarde du secret ; RS 510.413)
[59] La restriction actuelle de la procédure de sauvegarde du secret aux contrats dont le contenu est classifié du point de vue militaire est abrogée par l'entrée en vigueur de la loi sur la sécurité de l'information.

confère pas automatiquement le droit de se voir attribuer un mandat. L'adjudication reste le choix du mandant. Ces contrôles sont réalisés selon les directives du standard NIST 800-151 « Third Party Personnel Security » (PS-7).
La LSI permet désormais aussi de soumettre des personnes qui doivent exploiter, gérer, entretenir ou contrôler des systèmes d'information critiques de la Confédération (ou certaines parties de ces systèmes) à des contrôles de sécurité relatifs aux personnes.

Mesures à la conception du contrat : conformément à l'OPCy, les unités administratives s'assurent qu'en cas d'acquisition de prestations auprès d'un fournisseur externe, les directives en matière de sécurité informatique font partie intégrante du contrat. À cet égard, le document « Référence aux directives en matière de sécurité informatique de l'administration fédérale pour les documents d'appel d'offres »[60] a été élaboré pour soutenir les unités administratives. Il contient des blocs de texte, qui peuvent être intégrés aux documents d'appel d'offres officiels (en particulier pour les achats de logiciels informatiques), adaptés ou complétés en fonction des cas, par exemple dans un modèle de cahier des charges.
Les contrats de la Confédération contiennent toujours les Conditions générales (CG) de la Confédération correspondant au type du contrat. Les dérogations aux CG ne sont accordées qu'à titre exceptionnel et lorsque cela est justifié. Ces CG existent pour les prestations de service, les mandats de recherche, les achats de biens et pour divers actes juridiques. Elles contiennent également des dispositions relatives à la sécurité. La sécurité dépend néanmoins fortement des clauses convenues dans le contrat.
Les services d'achats de la Confédération doivent accorder un intérêt particulier à la sécurité de l'information chez les partenaires commerciaux de l'administration fédérale. La Conférence des achats de la Confédération (CA) met à la disposition des services d'achats de l'administration fédérale un modèle de clause pour les projets de contrat d'acquisition qui mentionne la protection des systèmes TIC contre les attaques ainsi que l'obligation de notification correspondante[61]. Le modèle de clause est conçu comme une disposition contractuelle indépendante et peut être intégré au contrat d'acquisition. L'objectif est de protéger autant les données et les informations que les systèmes contre et lors des cyberattaques visant les partenaires contractuels de l'administration fédérale. Dans le cas où un fournisseur ou prestataire de l'administration fédérale est victime d'une cyberattaque, l'entreprise concernée doit immédiatement et directement en informer les mandants de la Confédération et prendre des mesures immédiates après concertation avec eux. Le modèle de clause est particulièrement adapté aux acquisitions qui présentent un risque de cyberattaque élevé. L'application de la clause est évaluée en fonction des besoins et adaptée aux rapports concrets. Une conception individuelle des risques doit être convenue pour chaque contrat.

Une conception méticuleuse du contrat permet ainsi de couvrir de nombreux aspects de la sécurité et la Confédération peut se réserver des droits de contrôle. En pareil cas, la Confédération ne peut toutefois pas faire valoir ses besoins en matière de sécurité de manière régalienne (unilatérale) comme dans la procédure de sauvegarde du secret, mais doit, le cas échéant, engager une procédure civile. armasuisse, en sa qualité de service d'achats compétent, règle la gestion et les prescriptions de traitement des informations dignes de protection dans les arrangements contractuels pour les acquisitions de l'armée.

4.2 Application de standards dans les infrastructures critiques

Comme nous l'avons vu dans le chapitre 3.2, les directives légales concernant l'application de standards de la sécurité des produits et de la SCRM dans les infrastructures critiques sont peu nombreuses.

[60] Voir la newsletter septembre 2020 de la Conférence des achats de la Confédération (CA)
[61] Voir la Clause contractuelle type (et les explications) de la CA pour les cyberrisques

Néanmoins, il ne faut pas sous-estimer l'importance des standards pour les entreprises des secteurs critiques. Les standards sont souvent utilisés comme des guides essentiels pour la mise en œuvre de mesures et aident les entreprises internationales à coordonner leur cybersécurité par-delà les frontières. Le présent chapitre aborde en premier lieu l'importance des standards dans les infrastructures critiques et montre le rôle qu'ils jouent dans le domaine de la sécurité des produits et de la SCRM, malgré une législation qui n'impose leur application qu'à de rares cas. La Confédération encourage l'application de standards par des analyses des risques systématiques dans les secteurs critiques et en apportant un soutien spécialisé à l'élaboration de standards minimaux pour les TIC. Ces deux mesures sont également brièvement décrites dans ce chapitre.

4.2.1 Évaluation générale de l'application des standards dans les infrastructures critiques

Beaucoup d'entreprises appliquent leurs mesures de sécurité informatiques sur le modèle des standards internationaux, malgré leur caractère non contraignant. L'étude « TÜV-Cybersicherheitsstudie » de 2019 réalisée en Allemagne confirme que c'est le cas pour 64 % des entreprises interrogées[62]. La situation en Suisse est probablement comparable. Selon une étude sur la cybersécurité dans les PME suisses, 60 % d'entre elles s'appuient sur des standards internationaux[63]. Il s'agit de toute évidence d'une approche pragmatique pour renforcer la sécurité des TIC en utilisant les standards comme des directives ou des outils. Une mise en place complète et certifiée n'est pas recherchée. C'est pourquoi l'estimation du nombre d'exploitants d'infrastructures critiques qui appliquent des standards est compliquée. Afin de mieux cerner cette question, l'Office fédéral pour l'approvisionnement économique du pays (OFAE) a interrogé ses experts sur l'importance des standards dans leur branche[64]. Ceux-ci confirment que les standards relatifs à l'application sûre des moyens TIC sont connus de la plupart des entreprises qui les appliquent selon leurs besoins. Selon ces experts, ce sont les standards de type ISO que les entreprises suisses trouvent le plus pertinent. Les experts font remarquer que l'application des standards se limite à l'aspect procédural et technique. Les tests physiques du matériel ou les analyses du code source des logiciels dépassent largement les ressources financières et en personnel disponibles dans les entreprises selon les déclarations des experts.

En ce qui concerne la SCRM, peu d'entreprises ont recours à une gestion des fournisseurs systématiques axée sur la sécurité de l'information. Certaines entreprises définissent des critères d'évaluation liés à la sécurité et intègrent systématiquement les risques de la gestion des fournisseurs dans la gestion des risques de l'entreprise. Il s'agit typiquement d'entreprises plutôt importantes et financièrement solides ainsi que d'entreprises particulièrement exposées.

4.2.2 Analyses des risques dans les secteurs critiques

Les risques et les vulnérabilités des secteurs critiques sont régulièrement analysés par des experts de l'économie et de la gestion dans le cadre de l'application de la SNPC et de la stratégie de protection des infrastructures critiques (PIC). L'accent est notamment mis sur les cyberrisques. Les résultats obtenus aident à mieux organiser les cyberrisques spécifiques aux infrastructures critiques, déduire les mesures correspondantes et les prioriser.

Toutes les analyses de risques et de vulnérabilités déjà effectuées sont actualisées et de nouvelles mesures de résilience sont déduites dans le cadre de la deuxième SNPC 2018-2022. Cette entreprise est coordonnée par l'Office fédéral de la protection de la population (OFPP). Les mesures de résilience prises pendant la période couverte par la première SNCP et celles en cours sont prolongées selon les responsabilités définies.

[62] TÜV Cybersicherheitstudie 2019
[63] Cyberrisiken in Schweizer KMU, gfs Zürich, 2017
[64] L'enquête a été réalisée en juin 2019.

4.2.3 Standards minimaux, manuels et directives

L'OFAE a mis au point un standard minimal pour améliorer la résilience informatique[65]. Ce standard minimal se base sur le standard NIST et doit servir de recommandation et de principe directeur aux exploitants d'infrastructures critiques pour améliorer la résilience informatique (SCRM incl.). L'OFAE développe en collaboration étroite avec les secteurs des standards et des directives spécifiques au secteur sur la base du standard minimal général[66].
Les standards minimaux ne sont pas juridiquement contraignants et présentent l'avantage de pouvoir être intégrés dans les structures établies dans les secteurs. Les directives techniques développées dans les secteurs sont appliquées et respectées depuis de nombreuses années. Les compléter avec des directives en matière de sécurité informatique pourrait avoir un effet conséquent sur la sécurité dans le secteur.

5 Bilan

Les défis des domaines de la sécurité des produits et de la SCRM dans la cybersécurité et la cyberdéfense sont considérables. Les risques liés à un manque de sécurité des produits et ceux en lien avec les fournisseurs peuvent être réduits, mais ne peuvent pas être évités. Ces deux aspects concernent des éléments majeurs de la protection contre les cyberrisques. Identifier les mesures pour faire face à ces défis est par conséquent de la plus haute importance. L'application de standards reconnus internationalement peut également jouer un rôle important.
L'analyse des standards existants a montré l'existence de nombreux standards dans le domaine de la sécurité des produits et de leur utilisation sûre. Cela s'explique par le fait que les problèmes de sécurité des produits TIC sont connus depuis de nombreuses années. Plusieurs de ces standards de la sécurité des produits sont également appliqués dans une large mesure.
Les directives en matière de gestion des risques de la chaîne d'approvisionnement dans le domaine de la cybersécurité sont nettement moins développées. D'une part, ce n'est que récemment que les organismes de standardisation se sont intéressés au sujet. Ce n'est qu'une fois que la possibilité d'influence des États sur les fournisseurs stratégiques pour des intérêts géopolitiques a été reconnue que les risques des chaînes d'approvisionnement sont devenus préoccupants. D'autre part, le mélange des aspects techniques, juridiques et politiques complique les projets de standardisation. Étant donné la difficulté à déterminer le moment où un risque de la chaîne devient trop important, la plupart des standards de la SCRM se concentrent sur les processus et méthodes qui leur confèrent plus le caractère d'instructions recommandées que de normes contraignantes.
Le présent rapport a analysé comment la Suisse gère les standards internationaux dans les domaines étudiés, du point de vue de l'administration fédérale et de l'armée, mais aussi des infrastructures critiques. Les résultats de cette analyse sont résumés ci-dessous.

5.1 Le rôle des standards dans l'administration fédérale et l'armée

Les directives en matière de sécurité et d'utilisation sûre des produits TIC sont nombreuses au sein de l'administration fédérale et de l'armée. Le système des directives se base en grande partie sur les standards ISO/IEC de la suite 2700x et leur application dans les standards BSI. Ces directives disposent d'une nouvelle base légale depuis l'entrée en vigueur de l'OPCy en 2020. L'analyse annuelle réalisée par le NCSC à l'attention du Conseil fédéral sur l'état de la mise en œuvre de la sécurité des TIC dans

[65] Norme minimale pour les TIC (admin.ch)
[66] Normes minimales par secteur (admin.ch)

la Confédération montre que le travail en ce qui concerne la création de directives est loin d'être terminé. L'application de standards est délicate et demande un engagement continu. Pour conclure sur la situation de l'administration fédérale concernant les normes de sécurité des produits, il peut être constaté que l'accent doit être davantage mis sur une mise en œuvre globale et continue des directives ainsi que sur leur contrôle, plutôt que sur le développement du cadre global en grande partie déjà établi. Chaque année, le Conseil fédéral prend connaissance de l'état de mise en œuvre des directives de sécurité informatique et en informe en détail les commissions compétentes du Parlement.

L'administration fédérale et l'armée n'appliquent pas les standards du domaine de la SCRM dans la même mesure. Certains services disposent de quelques directives pour la mise en œuvre de la SCRM, cependant aucun cadre n'en impose la mise en œuvre systématique. Cela s'explique d'une part par le fait qu'il n'y a que quelques standards de la SCRM qui peuvent être directement mis en œuvre. Cela est dû d'autre part au cadre juridique. Les différentes étapes de la SCRM s'appuyaient auparavant sur des lois différentes. La loi sur la sécurité de l'information (LSI), qui n'est pas encore entrée en vigueur, mettra en place un cadre juridique uniforme pour les différentes mesures. Elle poursuit une approche intégrale en matière de sécurité des informations qui se compose de la protection des informations (protection de l'État), de la sécurité informatique, de la sécurité des personnes et de la sécurité de l'exploitation. En combinaison avec les principes de base fixés dans la LMP et les exceptions aux principes du libre-échange, il sera dorénavant déjà possible d'exercer une influence à un stade précoce (chaîne d'approvisionnement) de l'acquisition (p. ex. exclusion précoce de fournisseurs présentant des risques) et donc de mettre en place au sein de la Confédération un système de SCRM rigoureux.

5.2 Le rôle des standards dans les infrastructures critiques

Par rapport à la situation dans l'administration fédérale, peu de directives contraignantes pour l'application des standards de la sécurité des produits et la SCRM existent pour les infrastructures critiques. Les efforts se sont intensifiés dans de nombreux secteurs au cours des dernières années pour introduire de telles directives par l'intermédiaire d'accords sectoriels, de manuels ou de lignes directrices. L'introduction de standards dans les infrastructures critiques demeure toutefois incomplète, ces travaux ainsi que la mise en œuvre des directives reposant en grande partie sur le volontariat des entreprises. Le risque qu'un système mal protégé puisse nuire à la sécurité d'autres exploitants d'infrastructure subsiste en raison de l'interdépendance des infrastructures critiques due à la numérisation.

La création de nouvelles directives juridiquement contraignantes semble être la solution la plus évidente pour une meilleure généralisation des standards. L'existence de plusieurs standards dans le domaine de la sécurité des produits permettrait de s'appuyer sur ceux-ci. Des directives à l'attention des exploitants d'infrastructures critiques pour une gestion sûre des produits TIC seraient envisageables. Il convient d'examiner quelles directives il serait judicieux de développer selon le domaine. Il faut à cet égard tenir compte des différentes applications des produits TIC dans les infrastructures critiques et de la nécessité d'adapter les directives à ces contextes. Il est en outre possible de créer soi-même des directives pour la sécurité des produits TIC. C'est pourquoi des certifications des produits TIC sont généralement exigées dans les domaines d'application particulièrement importants. Le développement de tels schémas de certification avance également à grands pas dans l'UE[67]. L'inconvénient de ces directives réside dans l'ampleur de la procédure de certification, souvent trop importante. Réaliser des certifications et les renouveler demande beaucoup d'efforts financiers et de temps aux fabricants et acheteurs en raison de la complexité des systèmes TIC et de leurs mises à jour fréquentes. Dans le cadre de la mise en œuvre de la Stratégie nationale de protection contre les cyberrisques (SNPC), le Conseil fédéral vérifie quels domaines ont besoin d'être réglementés, détermine dans quelles instances la responsabilité en matière de réglementation incombe à la Confédération, et propose au Parlement, si nécessaire

[67] Voir la nouvelle stratégie de cybersécurité de l'UE : Nouvelle stratégie de cybersécurité de l'UE (europa.eu)

et si la Confédération est compétente, des modèles de directives contraignantes pour l'application de standards dans les infrastructures critiques[68].

En principe, des directives relatives à des mesures régulatrices pour la gestion des risques de la chaîne d'approvisionnement pourraient également être introduites. Le chap. 2.2.6 de la norme minimale pour les TIC[69] de l'OFAE fournit des exemples de consignes possibles en matière de SCRM. Il convient cependant de relever que les directives en matière d'infrastructures critiques dans le cadre de l'acquisition de prestations et de la constitution de relations avec les fournisseurs représentent une intervention régulatrice relativement importante, et il importe de clarifier au préalable dans quelles conditions la Confédération est en droit de les édicter. De telles solutions ne sont pas prioritaires dans la promotion de l'application de standards de la SCRM.

Il convient en général de vérifier comment les capacités d'analyse des produits et des processus de production qui conditionnent leur fabrication peuvent être améliorées. Cela correspond à l'une des demandes principales soulevées dans le White Paper « Supply Chain Security » d'ICTswitzerland. La Confédération salue les initiatives privées de développement des capacités concernées et de centres de contrôle pour les composants matériels et logiciels en Suisse. Elle est prête à mettre son expertise à disposition pour les soutenir.

[68] L'OFPP a été chargé, dans le cadre de la mesure 2 de la stratégie PIC 2018-2022, d'examiner la possibilité de créer une base légale pour édicter des directives intersectorielles pour les exploitants.

[69] Office fédéral pour l'approvisionnement économique du pays : Norme minimale pour les TIC (admin.ch)