6282-2017

RÉPUBLIQUE ET CANTON DE GENÈVE

Genève, le 20 décembre 2017

Le Conseil d'Etat

6282-2017

Conférence des directrices et directeurs
des départements cantonaux de justice
et police (CCDJP)
Maisons des cantons
Monsieur Hans-Jürg Käser
Président
Speichergasse
Case postale
3001 Berne

Concerne : stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022

Monsieur le Président,

Le projet de la Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022, que vous nous avez adressé pour consultation en date du 23 octobre 2017, nous est bien parvenu et a retenu toute notre attention. Vous trouverez ci-après la détermination de la République et canton de Genève à ce propos.

A titre liminaire, nous saluons la mise à jour de cette stratégie, compte tenu de la rapide évolution de la situation sur les plans technique et légal, ainsi que de la diversité des menaces et des acteurs impliqués (tant à l'origine du danger que pour les contre-mesures).

En premier lieu, et contrairement à ce qui est proposé dans la stratégie, nous ne considérons pas qu'il soit suffisant de garder simplement une structure décentralisée, même pilotée de façon plus ferme (chapitre 3). Nous préconisons la création d'une agence fédérale spécialisée dans la sécurité des systèmes d'information, de manière analogue à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France. Cette agence devra avoir la capacité de donner des ordres d'exécution aux différentes instances concernées de la Confédération et des cantons. Elle servira également d'organe de contrôle à l'échelle fédérale.

Afin de coordonner les tâches au niveau cantonal, notre Conseil préconise aussi d'encourager la création de comités cantonaux de sécurité de l'information, regroupant les différentes instances (administration cantonale, hôpital, université, transports régionaux, entreprises, industries, groupes professionnels, etc...) sous l'égide de l'exécutif cantonal. Ces comités *ad hoc* serviront de relais entre l'agence fédérale, les instances concernées et le tissu économique.

De manière générale, la stratégie telle que proposée souffre de certaines lacunes. Il s'agirait notamment :

- de prendre en compte les stratégies des groupes sectoriels des métiers et des cantons (par exemple : la Stratégie sécuritaire du canton de Genève – Vision 2030), de les consolider et de capitaliser sur celles-ci;

- de renforcer les liens, échanges et collaborations entre Confédération, cantons, administrations et groupes professionnels. À cet effet, un article analogue à l'article 4.9 de ce projet consacré à la collaboration internationale pourrait être proposé;

- de privilégier l'approche des menaces au niveau transverse et global :
  - l'augmentation continue des surfaces d'attaque, l'interdépendance et les interactions entre les axes et moyens d'attaque nécessitent d'avoir une vue globale des menaces, méthodes et techniques malveillantes associées. En effet, l'apparition massive de menaces multiformes, coordonnées et interopérables (telles que combinaison de dénis de service avec un ver informatique pour la propagation) implique d'élargir la vision;
  - à cet effet, il est crucial d'établir une pyramide de consolidation des menaces;

- de privilégier l'approche risques et vulnérabilités au niveau local, au moyen par exemple d'observatoires cantonaux (ou régionaux) d'évolution des risques. En particulier, il est nécessaire de prendre en compte le fait que les vulnérabilités et niveaux de risques dépendent des conditions locales et des spécificités des métiers impactés, et que les mesures ne peuvent donc se résumer à une approche globale;

- d'inclure une approche en lien avec les risques liés à l'intelligence économique, ainsi que les types d'attaques qui en découlent;

- du point de vue pratique, de tenir compte de la latence inévitable qui a lieu entre la concrétisation d'une capacité d'attaque et la mise en œuvre de moyens de défense adéquats contre cette capacité.

En outre, ce projet de stratégie ne prend en compte que de façon très lacunaire les besoins propres à une grande majorité du tissu économique suisse, à savoir les PME. À l'exception de rares mentions (article 3.3, par exemple), les PME ne sont pas incluses dans cette stratégie et le soutien à celles-ci est quasi inexistant dans le projet. A titre d'exemple, des notices telles que celles proposées par l'Office fédéral pour l'approvisionnement économique, mais orientées sur la cybersécurité et la gestion des cyberrisques, seraient bienvenues. Notre Conseil considère ainsi que la SNPC doit être cohérente à tous les niveaux et doit s'appliquer à toutes les structures étatiques, cantonales et économiques, et ce quelle que soit leur taille.

En ce qui concerne les articles proposés dans la SNPC, nous vous faisons part des remarques qui suivent.

Article 2.1.1 : Cyberattaques

Concernant « la désinformation et la propagande », il est indispensable de prendre en compte les aspects liés à la mise en œuvre du vote électronique en Suisse. La stratégie doit assurer que des doutes tels que ceux qui discréditent continûment les « machines à voter

US »[1], par exemple, ne puissent être utilisés contre les implémentations de vote électronique en Suisse.

Par rapport aux groupes cibles « Autorités » et « Économie » de l'article 3.3, nous préconisons de prendre en compte les notions de fraudes de grande ampleur, telles que détournements de fonds ou destruction de données bloquant toute transaction financière.

Article 2.1.2 : Erreurs humaines et défaillances techniques

L'article ne prend pas en compte l'étude et la résolution de scénarios d'« enchaînement des événements », comme par exemple la perte d'un disque qui entraîne la perte d'un serveur critique pour le fonctionnement du réseau, et ainsi de suite jusqu'à la paralysie totale d'une infrastructure.

Article 3.1 : Vision et objectifs stratégiques

Notre Conseil considère qu'un important objectif stratégique est manquant, à savoir « l'adaptation du cadre légal et statutaire » pour parer aux menaces et réagir aux attaques. À ce jour, il n'est pas possible à la Confédération d'imposer des mesures aux administrations cantonales ou aux entreprises.

En outre, un autre objectif est de s'assurer que l'entier des actions et mesures soient prises dans un but commun et réalisées en commun. Il est donc indispensable de s'affranchir d'une vision en silos.

Article 3.2 : Principes

Aucun des principes ne comporte l'aspect de conservation de preuves permettant de retracer une attaque ou un incident. La notion de traçabilité et d'imputabilité, ainsi que la mise en œuvre de méthodes, d'outils et d'analyses d'événements adaptés, doivent donc intégralement faire partie des principes.

Par ailleurs, conformément à notre commentaire sur l'article 3.1, le principe déclarant que l'Etat *peut* intervenir sur le plan réglementaire est insuffisant et doit donc être renforcé.

Article 3.3 : Groupes cibles

Notre Conseil apprécie l'entrée des PME dans le groupe cible « Économie » dans cette deuxième version de la SNPC, mais regrette que ce groupe ne soit pas davantage pris en compte ailleurs dans cette stratégie. Une simple PME touchée pourrait induire des effets en cascade ayant des conséquences sur toute la Suisse.

Article 4.1 : Acquisition de compétences et de connaissances

L'article ne définit pas clairement quelles sont les responsabilités. Il semble évident que les hautes écoles universitaires traitent de la recherche fondamentale et les hautes écoles spécialisées de la formation dédiée, mais il n'est précisé nulle part qui doit s'occuper des tâches plus prosaïques comme la veille technologique (bien qu'il semble que MELANI soit active sur le sujet).

Relativement à la mesure 2 : « Extension et encouragement de l'offre de formation », nous préconisons de favoriser à tous niveaux la formation continue, aussi bien dans le contenu de de l'enseignement que dans la possibilité par les entreprises de faciliter ce type d'acquisition de compétences.

Relativement à la mesure 3 : « Création de conditions-cadres », les PME devraient être encore une fois mentionnées, en proposant par exemple un organe d'aide et de conseil à

[1] Régulièrement, des audits des machines utilisées dans certains états des USA pour permettre aux citoyens de voter démontrent la très faible sécurité de ces appareils (voir par exemple : https://www.sciencesetavenir.fr/politique/election-americaine-soupcons-de-fraude-sur-le-vote-electronique-dans-certains-etats_108366).

leur attention. Par ailleurs, il faudrait étendre le cadre des intervenants aux fédérations d'entreprises et aux chambres patronales.

Article 4.2 : Situation de la menace

Le tableau d'ensemble de la situation devra contenir en permanence une situation des risques et des vulnérabilités majeures.

Relativement à la mesure 4 : « Extension des capacités », la possibilité d'enregistrer des traces doit être mentionnée. Cette possibilité doit être strictement cadrée et l'analyse limitée aux buts définis; cette analyse doit aussi être autorisée seulement à un organisme désigné, fédéral ou cantonal.

Article 4.3 : Gestion de la résilience

Cet article se focalise sur des mesures techniques visant la résilience des informations et néglige les mesures organisationnelles concomitantes, telles qu'un organe de gouvernance et de contrôle des acteurs concernés.

Par ailleurs, nous proposons de favoriser la résilience en minimisant le recours aux technologies de l'information et l'interopérabilité des systèmes en privilégiant, par exemple, les solutions locales sans recours à l'internet quand celui-ci n'est pas indispensable.

Article 4.4 : Normalisation et réglementation

La situation actuelle du droit international montre une tendance croissante à édicter des lois dont la portée est extraterritoriale. Cependant, ce projet de SNPC ne traite pas de ce problème majeur, notamment en ce qui concerne la protection des données.

En conséquence, nous souhaitons que la SNPC impose que certaines structures soient soumises *exclusivement* au droit suisse, en définissant un article de loi permettant d'interdire des fournisseurs soumis à la loi d'un pays offrant une protection insuffisante au sens de la loi fédérale sur la protection des données (LPD).

Notre Conseil propose que le domaine de gestion de crises soit intégré dans les normes et réglementations, permettant ainsi l'amélioration de son traitement par des règles spécifiques au contexte de la Suisse. Enfin, nous préconisons le renforcement de la participation de la Confédération dans les groupes internationaux de normalisation (tels que ceux de l'ISO) et d'alertes (notamment les équipes de réponse d'urgence aux attaques informatiques – CERT[2] et CSIRT[3]).

Article 4.5 : Gestion des incidents

Relativement à la mesure 12 : « Développement de MELANI en tant que partenariat public-privé », nous considérons qu'une structure de partenariat public-privé (PPP) ne peut pas tout résoudre. En effet, en cas de crise majeure, les responsabilités diluées par ce partenariat ne permettent pas d'agir efficacement et rapidement; elles rendent de surcroîts très probables des conflits de compétences. En conséquence, notre Conseil préconise une fois encore un organe de gouvernance et de contrôle qui puisse pallier ce problème.

La mesure 13 : « Offre de services destinés à toutes les entreprises » précise que le soutien de MELANI sera subsidiaire aux offres sur le marché. Si cette mesure était prise telle quelle, il en résulterait que les PME ne seraient pas prises en compte ; en effet, elles n'ont en général pas les moyens de s'offrir des outils du marché et MELANI n'aura pas les ressources pour les aider. Nous préconisons donc que l'offre de MELANI s'adapte aux besoins des clients et aux cibles potentielles.

---

[2] "Computer Emergency Response Team" ou "Computer Emergency Readiness Team"
[3] "Computer Security Incident Response Team"

Nous proposons également une mesure visant à travailler sur les principes de détection, de gestion et de traitement des signaux faibles, de leur analyse et de leur consolidation en une information utilisable par les parties concernées.

Article 4.6 : Gestion de crises

Relativement à la mesure 16 : « Exercices communs » et compte tenu de l'étendue potentielle d'une cybercrise, notre Conseil préconise que ces exercices incluent également des représentants de l'économie privée, y compris les PME, et ne se limitent pas exclusivement aux administrations et aux infrastructures d'importance vitale.

Il est bien connu qu'après un certain temps, les personnes sont épuisées et ne sont plus capables de traiter les informations et leurs tâches de manière adéquate. Nous proposons donc une mesure s'attachant à des recommandations de traitement et de capacités de résilience vis-à-vis d'une crise de longue durée.

Article 4.8 : Cyberdéfense

Relativement à la mesure 22 : « Capacités à mener des mesures actives », nous faisons remarquer qu'une défense active implique d'abord de déterminer les caractéristiques de l'attaquant. Les diverses recommandations relatives à la gestion des traces proposées dans notre prise de position n'en sont que plus indispensables.

Article 4.9 : Positionnement actif de la Suisse dans la politique internationale de cybersécurité

Par opposition aux « cybersconflits », une approche basée sur un soutien actif à la cyberpaix (telle que proposée par exemple par l'Union Internationale des Télécommunications) et la cyberdiplomatie devrait être mentionnée et explicitée plus en détails que dans cet article. Par ailleurs, de façon plus générale, le message de ce projet de SNPC gagnerait avec une approche plus positive et moins purement défensive.

Article 4.10 : Visibilité et sensibilisation

La mesure 25 : « Sensibilisation du public » se limite au grand public. Il conviendrait que les entreprises, et en particulier les PME, soient incluses dans cette mesure. Dans le cas contraire, les entreprises ne disposant pas de personnel spécialisé seraient dépendantes des compétences généralistes de leurs employés, compétences qui ne seront pas axées sur un même contexte.

Nous vous remercions de l'attention que vous prêterez à la prise de position de notre canton et vous prions de croire, Monsieur le Président, à l'assurance de notre haute considération.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :

Anja Wyden Guelpa

Le président :

François Longchamp