**REPONSE DU CONSEIL D'ETAT**

**à l'interpellation Florence Bettschart-Nabel –**
**Centre de Compétence Cyber : quelle plus-value pour les citoyens ?**

***Rappel de l'interpellation***

*Par communiqué de presse du 9 avril 2019, la Conférence latine des chefs de départements de justice et police (CLDJP) a annoncé avoir validé la création d'un Centre de compétence Cyber (CCC) romand piloté par les spécialistes de la police cantonale de Genève. Celui-ci assumera des compétences liées à l'accès aux données numériques, à l'évolution dans le cyberespace, à l'exploitation dans l'internet des objets des véhicules, ainsi qu'au processus d'exploitation et d'analyses du renseignement récolté.*
*Il est nécessaire de lutter contre la cybercriminalité, dont les chiffres sont en hausse constante ces dernières années. Selon la Conférence des commandants des polices cantonales, cette évolution est illustrée par l'augmentation des chiffres dans le domaine de l'escroquerie (+3060 infractions, +23 %), de l'utilisation frauduleuse d'un ordinateur (+627, + 13 %), de l'extorsion et du chantage (+ 316, +49 %), de l'appropriation illicite (+241, +9 %) et de l'introduction non autorisée dans un système de données (+187, +46 %).*
*Les citoyens sont particulièrement vulnérables face à ces attaques, tant il est difficile de faire face à la diversité d'infractions possibles (maliciels, hameçonnage, pourriels, rançongiciels, etc.).*

*Dans ce contexte, je prie le Conseil d'Etat de répondre aux questions suivantes :*

1. *Les citoyens pourront-ils directement s'adresser à ce CCC pour déposer plainte ou poser des questions ?*
2. *Ce CCC prévoit-il de faire des campagnes de prévention et d'information liées aux risques de la cybercriminalité ?*
3. *Quels seront les moyens financiers ou en ressources humaines, mis à disposition par l'Etat de Vaud dans ce CCC ?*
4. *Quelles sont les collaborations prévues avec le MELANI, la Centrale fédérale d'enregistrement et d'analyse pour la sûreté de l'information ?*

***Réponse du Conseil d'Etat***

En préambule, il est important de différencier les menaces dues à des actes illicites délibérés (cyberattaques) et les dangers dus à des événements provoqués de façon non intentionnelle (erreurs humaines et pannes techniques). Il a, en effet, été observé, ces dernières années, une forte augmentation des menaces dues aux cyberattaques ; il est donc important, vu la diversité des cyberattaques possibles, d'établir une distinction entre les différents phénomènes. Bien que les cyberattaques puissent se combiner ou se chevaucher, il est possible de distinguer cinq types de cyberattaques :

- Cybercriminalité: elle regroupe, au sens étroit du terme, les infractions pouvant être réalisées qu'au moyen de l'informatique, soit à l'aide d'outils informatiques ou en exploitant les vulnérabilités de ce moyen. Au sens large, elle rassemble les infractions qui auraient pu être commises sans recourir à des outils informatiques, mais pour lesquelles ces derniers ont été utilisés comme moyens d'action ou de supports de stockage (cyberescroqueries, notamment).
- Cyberespionnage: il s'agit d'une activité visant à obtenir des informations de manière non autorisée à des fins politiques, militaires ou économiques. Cette activité peut être pratiquée par des acteurs étatiques ou non étatiques.
- Cybersabotage et cyberterrorisme: ce moyen désigne une activité destinée à perturber ou à détruire le fonctionnement de l'informatique, ce qui peut également avoir des conséquences physiques en fonction de la nature du sabotage et de la cible attaquée.
- Désinformation et propagande: cela porte sur la menace due à la diffusion ciblée d'informations erronées ou obtenues illégalement par des cyberattaques dans le but de discréditer des acteurs politiques, militaires ou civils ; ce moyen gagne en importance.
- Cyberconflits: Si le scénario d'une guerre menée exclusivement dans le cyberespace (cyberguerre) est actuellement considéré comme peu réaliste, il est avéré en revanche que des cyberattaques de toutes sortes sont utilisées comme des moyens de guerre dans divers conflits.

Outre les cyberattaques ciblées et délibérées, il est également possible que des actes involontaires ou des événements liés aux conditions naturelles et techniques provoquent des dégâts touchant le cyberespace ou l'environnement physique.

Ainsi, toutes les réponses à ces cyberrisques, qu'il s'agisse d'attaques ou de pannes constituent ce que l'on appelle la cybersécurité. La cybersécurité est donc l'ensemble des techniques, politiques et pratiques sociales permettant de répondre à la prolifération des risques numériques caractérisant les sociétés contemporaines, incluant les diverses formes de délinquance numérique. Conscient de ces risques, le Conseil d'Etat a, tant dans son programme de législature 2017-2022 que dans le cadre de sa stratégie numérique adoptée en novembre 2018, souligné la nécessité d'assurer la sécurité de la population et des entreprises. A ces fins, plusieurs services de l'Etat contribuent à la sensibilisation, à l'information et à la prévention des cyberrisques.

La cybercriminalité implique en revanche une réponse des autorités de poursuite pénale à certains actes illicites délibérés. Cette réponse doit aujourd'hui être adaptée. Le cyberespace fournit aux criminels potentiels de nouvelles opportunités, susceptibles d'entraîner de sérieux dommages pour la société et l'économie. Les actes ne sont plus véritablement limités dans le temps et l'espace. En effet, la cybercriminalité se joue des frontières territoriales, dans un processus hautement dynamique aux cycles d'innovation très courts.

Par conséquent, face à cette évolution, il est urgent de rechercher de nouvelles solutions en matière de poursuite pénale. Il convient d'agir dans toute la Suisse et en collaboration avec des partenaires internationaux, afin d'améliorer l'interopérabilité et la capacité de réaction ainsi que de coordonner efficacement les compétences professionnelles, techniques et humaines, sans devoir pour autant céder des prérogatives d'une autorité ou d'un niveau étatique à l'autre.

C'est donc dans ce contexte précis que la création du « réseau de soutien aux enquêtes relatives à la cybercriminalité » constitue une des quatre mesures judiciaires de la nouvelle stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022 (SNPC 2). La Confédération (fedpol) et les cantons (Conférence des directrices et directeurs des départements cantonaux de justice et police, CCDJP) élaborent une convention administrative sur la collaboration et la coordination entre le centre de cybercompétence national (National

Cyber Competence Center actif NC3) et les centres de cybercompétence régionaux (Cyber Competence Centers RC3) dans le cadre du réseau de soutien aux enquêtes relatives à la cybercriminalité.

Le centre de cybercompétence régional genevois, dont il est question dans cette interpellation, fait partie de ce réseau.

Suite à ce préambule, le Conseil d'État répond aux questions de la manière suivante :

1. *Les citoyens pourront-ils directement s'adresser à ce CCC pour déposer plainte ou poser des questions ?*

Le dispositif concordataire prévoit que seules des situations extraordinaires soient traitées par le centre de compétence cyber romand, qui lui-même s'inscrira dans un réseau de centres de compétence régionaux (GE, BE, ZH, SG), dont fera également partie le centre de compétence national de la Police fédérale (fedpol). Ce réseau de soutien aux enquêtes relatives à la cybercriminalité (appelé NEDIK sur le plan national) est en cours de formalisation et il est possible que chacun d'eux se spécialise dans une ou plusieurs problématiques spécifiques. Ce point est en discussion au niveau de la Conférence des directrices et directeurs des Départements cantonaux de justice et police (CCDJP).
Les cantons seront donc la porte d'entrée habituelle pour les citoyens. Une fois la plainte déposée, elle suivra le processus judiciaire pouvant déboucher sur l'ouverture d'une instruction pénale. Le cas échéant, elle pourra faire l'objet d'une demande d'appui et/ou de prise en charge par le centre de compétence cyber romand (ou autre selon les spécificités) dans la phase d'investigation policière ou suite à l'ouverture d'une instruction par le Ministère public compétent.
Concernant les questions, il s'agira de procéder par analogie, les centres régionaux ou le centre national étant consultés via les cantons en fonction de leurs sphères de compétences spécifiques.

2. *Ce CCC prévoit-il de faire des campagnes de prévention et d'information liées aux risques de la cybercriminalité ?*

Oui, il participera pour ce qui relèvera de sa compétence aux campagnes qui seront lancées régulièrement tant au niveau régional que suisse. Nous pouvons mentionner ici la nouvelle campagne nationale dont les cantons romands ont été les instigateurs. Des campagnes ou des outils de prévention continueront également à être développés au niveau cantonal par les entités en charge de ces questions à l'Etat de Vaud. A titre d'exemple, on peut citer les actions de sensibilisation des entreprises aux risques de sécurité numérique et aux bonnes pratiques mises en place par la DGNSI. Un autre exemple est la campagne de prévention menée par le DFJC contre le cyberharcèlement. Dans le cadre de l'introduction de l'éducation numérique dans tous les systèmes de formation vaudois (du primaire au secondaire II), il fournit aux jeunes des connaissances de base et des réflexes de prudence nécessaires à la bonne utilisation des outils numériques.

3. *Quels seront les moyens financiers ou en ressources humaines, mis à disposition par l'Etat de Vaud dans ce CCC ?*

Le canton de Vaud participe à hauteur de 30% selon la clé de répartition romande. Il finance donc, à ce taux, d'une part les deux postes concordataires attribués au CCC situé à Genève, validés par la Conférence latine des chefs des Départements de justice et police (CLDJP), et d'autre part, à l'hébergement de l'outil informatique PICSEL à Neuchâtel selon la même clé de répartition.

4. *Quelles sont les collaborations prévues avec le MELANI, la Centrale fédérale d'enregistrement et d'analyse pour la sûreté de l'information ?*

La Police cantonale vaudoise et plus particulièrement la police de sûreté s'est réorganisée récemment en réponse aux menaces en matière de cyber criminalité. La direction de la police de sûreté a décidé de centraliser la prise en charge des plaintes cyber et de créer une nouvelle division enquêtes cyber (DEC), qui a été rattachée à la brigade traces technologiques (BATT). Son effectif de 7,4 collaborateurs, en provenance de la brigade financière et des régions judiciaires, a été déployé au mois d'avril 2019 dans le cadre des mutations annuelles.
Cette division qui concentre l'ensemble du traitement des affaires cybercriminelles, à l'exception de la pédopornographie dévolue à la division moeurs, est désormais l'interlocuteur privilégié des partenaires actifs dans ce domaine, dont bien évidemment MELANI, au même titre que les unités dédiées au sein de l'office

fédéral de la police (fedpol), des autres cantons romands et suisses et des actuels ou futurs CCC régionaux (RC3) ainsi que du centre national (NC3).
Nous précisons encore que la création des centres des compétences cyber s'inscrit dans le dispositif national de lutte contre la cybercriminalité de la Conférence des commandants des Polices cantonales de Suisse (CCPCS), qui a été repris dans la nouvelle stratégie nationale de protection de la Suisse contre les cyberrisques 2018 – 2022 (SNPC 2 – annexée), sous la forme des mesures 18 à 21. Certaines de ces mesures ont déjà été mises en œuvre, notamment la mesure 20 (Formation à la lutte contre la cybercriminalité), par un e-learning suivi par l'ensemble de policiers suisses (environ 20'000 personnes) et la création d'une formation de base spécifique pour les enquêteurs cyber (5 jours), tous deux sous l'égide de l'Institut suisse de police (ISP). Ces formations constituent le socle sur lequel les processus coordonnés de traitement des cas cybercriminels sont aujourd'hui construits, à l'instar du réseau de soutien aux enquêtes relatives à la cybercriminalité (NEDIK) qui fait l'objet de la mesure 19.

En conclusion, la création d'un centre de compétence cyber au niveau romand est un dispositif pertinent et nécessaire pour pouvoir lutter dans les meilleures conditions qui soient contre les infractions cyber qui devraient malheureusement augmenter ces prochaines années. Il s'inscrit parfaitement dans le réseau national de lutte contre la cybercriminalité.

Ainsi adopté, en séance du Conseil d'Etat, à Lausanne, le 11 septembre 2019.

| La présidente : | Le chancelier : |
| --- | --- |
| *N. Gorrite* | *V. Grandjean* |

**ANNEXES**

- Communiqué de presse

**POLICES SUISSES**

SKPPSC
Schweizerische Kriminalprävention
Prévention Suisse de la Criminalité
Prevenzione Svizzera della Criminalità

## COMMUNIQUÉ DE PRESSE

---

**Les polices suisses et la Prévention Suisse de la Criminalité s'associent pour la cyberprévention.**

**Le 17 juin 2019, une campagne nationale de prévention des cyberescroqueries démarre sur le thème « *Et vous ? Vous auriez dit oui ?* ». Les polices suisses et la Prévention Suisse de la Criminalité (PSC) unissent leurs forces afin de sensibiliser la population aux bons comportements à adopter sur internet.**

Ce lundi 17 juin, les quatre concordats policiers suisses (RBT, PKNW, ZPKK, ostpol), Zurich ainsi que PSC débutent une campagne nationale de prévention afin de sensibiliser la population aux potentiels risques présents sur Internet. Dans ce cadre, des capsules vidéos d'environ une minute chacune seront diffusées sur les réseaux sociaux, au rythme d'une par trimestre. Les trois thèmes abordés en 2019 seront les escroqueries sur les plateformes de petites annonces (www.skppsc.ch/cyberescroqueries), l'escroquerie sentimentale *(Romance scam)* ainsi que les mules financières (*Money Mule)*. Les diffusions se poursuivront en 2020 avec de nouvelles escroqueries abordées. Diverses autres actions de sensibilisation seront entreprises en parallèle dans les cantons (campagne d'affichage, distribution de cartes postales, articles de fond diffusés sur les sites dédiés à la prévention, conférences, etc.).

« *Et vous ? Vous auriez dit oui ?* »

Cette nouvelle campagne mettra en exergue la dichotomie entre le comportement des citoyens dans la vie réelle et leur comportement sur Internet. En effet, dans une même situation, la majorité des gens semble agir différemment sur Internet ou dans la "vraie" vie. Certaines attitudes mènent bien souvent à une cybervictimisation, avec des conséquences financières et psychologiques très lourdes. L'objectif est également de transmettre quatre conseils généraux quant aux comportements de base à adopter sur Internet afin de minimiser le risque d'être victime d'un escroc :

- *Ne vous fiez jamais à une personne que vous ne connaissez que par Internet.*
- *Ne transmettez jamais de mots de passe et de documents officiels (passeport, permis de conduire, etc.).*
- *Ne divulguez jamais de photos ou d'informations intimes.*
- *Ne versez jamais d'acompte sans être sûr de la fiabilité de votre interlocuteur.*

Cette coordination nationale s'avère nécessaire en raison de l'augmentation croissante des cas de cybercriminalité au fil des ans. En effet, bien que les cas de cyberescroqueries ne fassent généralement pas encore l'objet d'un décompte spécifique de la part de l'Office Fédéral de la Statistique (OFS) et des polices, les statistiques nationales 2018 montrent une augmentation de 23% des escroqueries, une grande partie de cette hausse pouvant être attribuée au cyber. De plus, les enquêtes judiciaires consécutives aux dépôts de plaintes des nombreuses victimes s'avèrent souvent complexes, en raison du caractère international d'Internet.

Lausanne, le 17 juin 2019

**Polices du concordat Romandie, Berne et Tessin :** Com princ Jean-Christophe Sauterel, chef Conférence Information et Prévention, 021 644 80 22 / 079 705 29 91