GRAND CONSEIL

**JANVIER 2025** **RC-22_RAP_20**

# RAPPORT DE LA COMMISSION THÉMATIQUE DES SYSTÈMES D'INFORMATION chargée d'examiner l'objet suivant :

## Rapport du Conseil d'État au Grand Conseil sur le Postulat David Raedler et consorts – Les pirates sont informatisés et ne se limitent plus au Léman : agissons à tous les échelons face aux cyberattaques (21_POS_44)

## 1. PRÉAMBULE

La Commission thématique des systèmes d'information (CTSI) s'est réunie le mardi 10 décembre 2024 à la salle du Bicentenaire, Place du Château 6 à Lausanne, pour traiter de cet objet.

Elle était composée de Mmes et MM. Maurice Gay (président et rapporteur), Céline Baux, Carole Dubois, Olivier Gfeller, Sabine Glauser Krug, Yann Glayre, Didier Lohri, Laurent Miéville, Charles Monod, Yves Paccaud, Cédric Roten, Michael Wyssa, Regula Zellweger, Valérie Zonca.
Excusé·es : Théophile Schenker (remplacé par S. Glauser Krug), Vincent Jaques (remplacé par Y. Paccaud).

Mme Nuria Gorrite, cheffe du était excusée. Avec l'accord préalable du président de la commission, elle avait délégué les collaborateurs suivants de son administration qui ont participé à la séance : MM. Patrick Amaru, directeur général de la Direction générale du numérique et des systèmes d'information (DGNSI) et Marc Barbezat, directeur de la sécurité des systèmes d'information à la DGNSI et délégué à la cybersécurité.

M. Yvan Cornu, secrétaire de la commission, a tenu les notes de séance et contribué à la rédaction de ce rapport de commission, ce dont nous le remercions.

## 2. POSITION DU CONSEIL D'ÉTAT / DE LA DIRECTION GÉNÉRALE DU NUMÉRIQUE ET DES SYSTÈMES D'INFORMATION (DGNSI)

Le Conseil d'État reste effectivement préoccupé par les cyberattaques qui font d'ailleurs régulièrement les gros titres dans les médias. Le postulat avait été déposé en 2021 au moment des attaques de la commune de Rolle, puis de la ville de Montreux. Depuis lors, beaucoup de choses ont été mises en place en termes de cybersécurité.

À partir de 2013 déjà, l'État de Vaud a investi afin de protéger et sécuriser le périmètre informatique de l'administration cantonale vaudoise (ACV). Dès 2021, la stratégie de sécurité s'est étendue aux communes et aux entités parapubliques avec lesquelles l'ACV a des échanges réguliers. L'objectif est de soutenir ces partenaires afin de renforcer leur capacité à faire face aux menaces numériques et de garantir la continuité des services essentiels.

Une convention de cybersécurité a été signée le 4 juillet 2023 pour renforcer la cybersécurité des 300 communes vaudoises et d'environ 130 associations intercommunales. Dans ce cadre, il est à relever la création de la force cantonale d'intervention cybersécurité (CSIRT pour Computer Security Incident Response Team) née d'une volonté politique du Canton et des communes. Celle-ci est opérationnelle depuis le 1er janvier 2024 et développe ses services sur 3 axes principaux : la cyberréaction ; la cyberrésilience et la cyberprévention.

Les premiers retours, après quelques mois d'exploitation, sont plutôt positifs. Progressivement, la force de cybersécurité du Canton se déploie sur tout un réseau de partenaires, même des institutions privées comme pour Vidymed qui a subi une cyberattaque début décembre 2024 et a mis en place une cellule de crise en collaboration avec la force cantonale d'intervention cybersécurité (CSIRT).

Le directeur la DGNSI tient à relever l'effort particulier mis sur la formation, la sensibilisation et la prévention, l'objectif étant de renforcer la conscience et les bonnes pratiques face aux risques de cybersécurité. Cette année, la DGNSI a mené une campagne de sensibilisation au risque de phishing auprès de plus de 47'000 destinataires (le personnel de l'ACV, les enseignant·es, les collaboratrices et collaborateurs du CHUV et d'Unisanté, également auprès des député·es).

La stratégie de cybersécurité est en phase de finalisation et devrait être publiée au premier trimestre 2025.

**Mutualiser les forces**

Le délégué à la cybersécurité insiste sur la devise « ensemble, plus fort ». Par rapport au postulat, il relève l'importance du lien et des coopérations avec la Confédération. Des échanges existent aussi avec les autres cantons. Il adhère également à la proposition d'établir un standard minimum de cybersécurité qui est d'ailleurs en cours d'élaboration par la force cantonale d'intervention cybersécurité (CSIRT), en étroite collaboration avec les communes. L'établissement d'un standard minimum de cybersécurité constitue pour le Conseil d'État une étape clé pour renforcer la stratégie de sécurité du Canton et protéger les communes contre les cybermenaces. En outre, les outils, les formations et les bonnes pratiques développés pour le Canton sont mis à disposition des communes, afin d'assurer une cohérence et une efficacité maximales dans la gestion de la cybersécurité.

Il existe aussi des collaborations régulières dans le domaine de la lutte contre la cybercriminalité avec les acteurs académiques majeurs établis sur notre territoire, à savoir l'EPFL (École polytechnique fédérale de Lausanne), l'UNIL (Université de Lausanne) et l'HEIG-VD (Haute école d'ingénierie et de gestion du Canton de Vaud).

## 3. POSITION DU POSTULANT

Le postulant trouve le rapport du Conseil d'État intéressant tant au niveau des réponses à ses questions qu'au niveau de la ligne stratégique développée. Les cyberattaques de Rolle, puis de Montreux, avaient mis en évidence que les communes n'étaient pas forcément bien préparées pour éviter les attaques et certainement insuffisamment outillées pour y répondre.

En 2021, on savait déjà que le Conseil d'État avait pour vision de renforcer les collaborations avec les communes en termes de cybersécurité. Au niveau fédéral, la décision avait aussi été prise de transformer le Centre national pour la cybersécurité (NCSC) en un Office fédéral de la cybersécurité (OFCS), à compter du 1er janvier 2024. Les dispositions fédérales – notamment, la stratégie nationale de protection de la Suisse contre les cyber-risques (SNPC) – imposent de prendre des mesures au niveau cantonal et communal.

L'OFCS met en évidence le fait que la situation s'aggrave chaque année ; sa statistique hebdomadaire montre que le nombre de cyberincidents signalés ne cesse d'augmenter.[1] Le nombre de cas d'hameçonnage (phishing) annoncé a une nouvelle fois progressé de près d'un tiers en 2024 par rapport à l'année précédente. En conséquence, il est impératif d'agir ; le postulant souligne que dans ce domaine « on n'a pas le temps et perdre du temps ». Comme cela ressort du rapport, il convient de coordonner les actions au niveau fédéral, cantonal et communal, pour faire face à des organisations professionnelles et spécialisées dans la cybercriminalité.

Le postulant relève positivement la création de la force cantonale d'intervention cybersécurité (CSIRT) qui répond précisément au point le plus urgent qui consistait à venir en aide aux communes, du fait notamment qu'elles traitent beaucoup de données sensibles.

[1] https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2024/wochenrueckblick_52.html

Il se réjouit que le Conseil d'État encourage la collaboration entre la Confédération et les cantons, par le biais du Réseau national de sécurité (RNS), afin d'assurer l'alignement des stratégies. Une collaboration étroite est entretenue sur divers sujets, tels que la sensibilisation auprès des communes ou l'établissement de standards minimaux, en veillant à éviter les redondances.

**Stratégie de cybersécurité et standards minimaux de cybersécurité attendus en début 2025**

Le postulant émet deux réserves sur ce rapport :

- le temps pris pour répondre au postulat, alors même que la rapidité des mesures à mettre en place face aux cyberattaques et à la cybercriminalité est un élément décisif ;
- le fait que les deux éléments centraux et prioritaires, à savoir la stratégie de cybersécurité et les standards minimaux de cybersécurité[2], sont encore en cours d'élaboration au moment de la publication de ce rapport. Annoncés d'ici à fin 2024, ces éléments sont attendus pour le premier semestre 2025. Le postulant souhaite que leur publication ne soit pas repoussée par le Conseil d'État.

**Formation et mesures préventives**

Pour illustrer la complexité du problème, le directeur de la DGNSI explique qu'il est extrêmement rare de retrouver les personnes coupables de cyberattaques du fait qu'elles proviennent exclusivement de l'étranger. Les attaques sont de plus en plus sophistiquées. Concernant les actions pour s'en prémunir, le directeur de la DGNSI insiste sur la rigueur dans la gestion des systèmes d'information et sur la formation des utilisatrices et utilisateurs. Cette culture de la sécurité doit arriver à maturité et cela prend du temps, même s'il faut effectivement agir vite face à la pression sécuritaire extérieure.

Il y a des vulnérabilités humaines et technologiques avec des entrées qui ne sont pas correctement sécurisées. Le délégué à la cybersécurité insiste sur l'authentification forte qui doit être un standard minimum et qui représente une barrière très efficace, sans laquelle la tâche des cybercriminels est grandement facilitée.

## 4. DISCUSSION GÉNÉRALE ET EXAMEN, PAGE PAR PAGE DU RAPPORT

**Actions de la force cantonale d'intervention cybersécurité (CSIRT)**

A ce jour, la force cantonale d'intervention cybersécurité (CSIRT) est peu intervenue directement. En mai 2024, un prestataire externe du Service des énergies de la ville d'Yverdon-les-Bains a subi une cyberattaque sur des compteurs électriques connectés. Lors de cet incident, une base de données a été piratée et exposée contenant des données personnelles de plus de 10'000 abonné·es du Service des énergies (données de contact et de facturation).

Néanmoins, la ville, victime collatérale ou indirecte de cette attaque, mais dont les systèmes informatiques n'étaient pas directement concernés, a relayé les informations concernant les risques et les bons conseils à suivre, établis par la force cantonale d'intervention cybersécurité (CSIRT).

Depuis sa création, la force cantonale d'intervention cybersécurité (CSIRT) a fait le tour des districts à la rencontre des syndics. De plus, le 5 décembre 2024, la DGNSI en collaboration avec l'État-major cantonal de conduite (EMCC) a conduit un exercice de simulation et de gestion de cybercrise auquel se sont inscrites près de 90 communes et associations intercommunales. Cela permet aux personnes de comprendre comment se déroule les étapes typiques d'une cyberattaque et de quelle manière réagir.

Parmi les 300 communes et les 130 associations intercommunales, il y a aujourd'hui un point de contact cybersécurité. Ce qui permet par exemple d'annoncer des vulnérabilités. Cela donne aussi la possibilité de monter une communauté active en matière de cybersécurité au niveau du Canton.

[2] L'établissement d'un standard minimum de cybersécurité constitue aussi pour le Conseil d'État une étape clé pour renforcer la posture de sécurité du Canton et protéger ses communes contre les cybermenaces.

**Exercices d'hameçonnage (phishing) : résultat insuffisant**

Une commissaire souligne l'importance de la prévention et rappelle que l'erreur humaine reste la cause principale des incidents. Elle demande si le comportement des utilisatrices et utilisateurs s'améliore au fil des campagnes de sensibilisation menées par la DGNSI. Au cours des années, les faux e-mails sont rédigés au plus proche d'un e-mail officiel et deviennent difficiles à détecter. L'IA va certainement rendre les faux e-mails encore plus difficiles à identifier.

Dans les exercices, la DGNSI s'adapte à l'évolution des cyberattaques, le but étant que les utilisatrices et utilisateurs réalisent où se cachent les risques. Lors de la 6e campagne de sensibilisation qui a eu lieu en novembre 2024, sur 47'000 e-mails malveillants envoyés près de 30% des destinataires n'ont pas détecté ce test et ont cliqué sur le lien. Pire, 11% des personnes ont même saisi un identifiant et un mot de passe. Les variations sont très importantes selon les services. Pour la DGNSI, ces résultats ne sont pas satisfaisants, d'autant qu'un seul clic malheureux peut provoquer un vol d'identité et favoriser ensuite une intrusion informatique. 90% des violations de données commence par là.

La personne qui cliquait sur le lien ou saisissait des données arrivait sur une page mentionnant qu'il s'agissait d'un phishing en indiquant les éléments qui auraient dû susciter leur attention et leur prudence. Mais les résultats restent anonymes. Il est prévu de continuer à former et expliquer ; la DGNSI va proposer un plan d'action pour sensibiliser sur les actions principales.

**Signaler un courriel indésirable**

L'humain est un rempart de sécurité efficace. Au niveau de l'administration cantonale vaudoise (ACV), il existe un bouton pour signaler tout e-mail suspect. Ces signalements permettent d'adapter immédiatement les filtres antispam. Une personne peut aussi alerter le centre opérationnel de sécurité (SOC) si elle réalise avoir cliqué par erreur sur un lien contrefait ou divulguer des données personnelles.

En revanche, les député·es n'ont pas d'option pour signaler un e-mail indésirable. Une députée a dû contacter le secrétariat du Grand Conseil afin de signaler cette tentative d'hameçonnage. Compte tenu de l'importance de la rapidité de réaction, elle préconise de mettre en place un tel bouton pour les député·es afin de pouvoir réagir immédiatement et de manière appropriée.

**Échanges d'informations sécurisés**

Un commissaire constate que des services de l'État ou des entités parapubliques communiquent de manière inadéquate en demandant des informations personnelles via des formulaires envoyés en pièces jointes ou des liens internet peu indentifiables. Les standards minimaux de cybersécurité devront s'appliquer. Le délégué à la cybersécurité met en avant les prestations de cyberadministration où la personne s'identifie de manière univoque et entre avec son identité électronique e-ID. Les échanges d'informations se font sur un portail sécurisé. De plus en plus, il y a la possibilité, pour l'État de Vaud, de signer des documents avec un cachet électronique.

L'utilisation généralisée de l'e-ID devra permettre d'augmenter le nombre de cyberprestations offertes par l'État de Vaud.

**Manque de formation spécifique en cybersécurité**

Concernant la volonté de l'État d'augmenter le nombre d'informaticiens en offrant 240 places supplémentaires au sein de la nouvelle École de Payerne, un commissaire relève que la cybersécurité n'est pas abordée au niveau du CFC. Ces notions sont acquises plus tard, dans des formations supérieures, au niveau HES ou EPF. Le commissaire préconise des formations de type ES dans le domaine de la cybersécurité dans le but d'avoir beaucoup de personnes formées dans ce domaine, actuellement en pénurie.

Après la maturité professionnelle, des apprenti·es continuent leur formation à la HEIG-VD à Yverdon. Des spécialisations se font aussi durant la carrière professionnelle. À l'interne, la DGNSI forme également du personnel à la cybersécurité ; les personnes proviennent de diverses filières.

**Droit à la déconnexion**

Pour une commissaire, la lecture de ce rapport donne le vertige ; la généralisation du numérique a généré une explosion des cyberattaques. On voit que des dispositifs très importants et coûteux doivent être mis en place tant pour se protéger que pallier ces attaques dont les conséquences peuvent se chiffrer en millions de francs ou avoir des conséquences considérables en termes de fuite de données sensibles.

Selon elle, les dispositifs de sécurité rendent l'utilisation des outils informatiques de plus en plus compliquée. En termes environnemental, on sait que l'interaction avec des IA qui nécessitent des serveurs très puissants va faire exploser la consommation d'énergie.

Face à ces constats alarmants, la commissaire propose, à contre-courant du passage au tout numérique, de miser sur le droit à la déconnexion soutenable d'un point de vue humain et social. Il faudrait considérer de se rendre moins dépendant du numérique.

Du côté de la DGNSI, il est répondu que les aspects de durabilité est prise en considération, notamment dans les certifications ISO. Il faut aussi se poser des questions sur la raison de collecter des données, moins je possède de données, moins je dois en protéger.

## 5. VOTES SUR LE RAPPORT DU CONSEIL D'ÉTAT (22_RAP_20)

À l'unanimité, la commission thématique des systèmes d'information (CTSI) recommande au Grand Conseil d'approuver ce rapport.

*Le rapporteur :*
*(Signé) Maurice Gay*

Nyon, le 10 janvier 2025