

CH++ demande la création d'un secrétariat d'État à la cybersécurité

Novembre 2021

L'évolution technologique rapide est un phénomène global qui ne s'épargne pas la Suisse. Notre pays doit réussir à maîtriser la transformation numérique et pour cela, il doit investir dans les infrastructures technologiques nécessaires. Cependant, cela modifie aussi les dangers potentiels : les cyberattaques représentent un énorme risque pour la sécurité, de la paralysie des services de base à la publication de données sensibles sur les citoyens. Les attaques récentes contre des communes, des hôpitaux et des services administratifs en ligne montrent que les cyberattaques constituent une menace systématique pour tous les domaines de la vie publique.

Au printemps 2018, la Confédération a adopté une stratégie nationale visant à protéger la Suisse contre les cyberrisques. Elle y mentionne notamment le niveau de menace fortement intensifié. Le *Centre national pour la cybersécurité* (NCSC), dirigé par le délégué fédéral à la cybersécurité, en est l'organe opérationnel. Le délégué fait à son tour rapport au chef du département fédéral des finances. Le « Groupe Cyber » coordonne la coopération avec les départements du DFF, du DFJP et du DDPS ainsi que la Conférence des commandants des polices cantonales de Suisse ; un comité de pilotage coordonne la coopération avec les unités administratives de la Confédération (telles que Armasuisse, la Chancellerie fédérale, etc.), les milieux économiques, les cantons et les universités. En mai de cette année, le NCSC comptait 32 employé-e-s ; treize postes vacants doivent encore être recrutés d'ici la fin de l'année.

En parallèle, le DDPS poursuit la stratégie « Cyber DDPS », qui a été adoptée en avril 2021. La Confédération y fait la distinction entre la *cyberdéfense* et la *cybersécurité*. La cyberdéfense désigne « les mesures de renseignement et de l'armée prises dans le but de protéger les systèmes critiques dont dépend la sécurité du pays, de se défendre contre les cyberattaques, de garantir la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberspace et de développer ses capacités et compétences afin

qu'elle puisse apporter un appui subsidiaire aux autorités civiles¹ » alors que cybersécurité constitue « l'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 effet² ».

Au vu de l'augmentation exponentielle des risques dans le domaine des cyberactivités, nous faisons trois constats principaux.

1. La cybersécurité doit être assurée pour tous les domaines de la vie publique : les cyberattaques viennent de partout et peuvent toucher tout le monde. Dans le secteur public, il n'est pas réaliste de s'attendre à ce que toutes les communes et tous les cantons soient constamment au plus haut niveau technologique en matière de cybersécurité. La Confédération doit donc être en mesure d'assurer la cybersécurité à tous les niveaux institutionnels et dans tous les domaines de la vie publique.

2. La sécurité est la base de la souveraineté numérique : il existe un besoin croissant pour une souveraineté numérique plus forte en Suisse (cloud, infrastructure de réseau critique, etc.). Sans la sécurité appropriée, cette souveraineté numérique est fondamentalement compromise.

3. Il est nécessaire de regrouper les ressources et les compétences : la cybersécurité nationale ne peut être garantie uniquement par un délégué fédéral à la cybersécurité et le nombre actuel de ses collaboratrices et collaborateurs. Les compétences en matière de cybersécurité des différents offices et départements doivent être regroupées au sein d'un nouveau secrétariat d'État à la cybersécurité doté de ressources suffisantes pour faire face à la menace croissante.

D'autres cyberactivités suivront sans aucun doute au niveau administratif. On peut partir du principe que toutes les activités dans le domaine de la cybersécurité seront fortement développées et croîtront en fonction des risques. En outre, il convient de noter que la cybersécurité touchera toutes les tâches de la Confédération, des cantons et des communes. Pour toutes ces raisons, la création d'un nouveau secrétariat d'État à

¹ <https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-83160.html>

² https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/strategie/Bericht_Umsetzungsstand_NCS_2018-2022_Mai_2019.pdf.download.pdf/Bericht_Umsetzungsstand_NCS_2018-2022_Mai_2019.pdf



la cybersécurité en tant qu'organe central est une mesure organisationnelle stratégique cruciale pour préparer la Suisse, sur le plan opérationnel, aux risques liés à la cybercriminalité en croissance rapide et en constante évolution ainsi que pour garantir la souveraineté numérique. Nous demandons à la Confédération de mettre cette mesure en œuvre le plus rapidement possible. Tôt ou tard, elle deviendra inévitable.