Conclusion

La problématique de la cybersécurité, en Suisse en général et dans le canton de Vaud en particulier, reste un sujet extrêmement important car les menaces qui planent sur les entreprises et les administrations publiques sont permanentes. L'annonce récente de la part des autorités Russes que la suisse était considérée comme un état hostile augmente encore ce risque. L'accroissement de la fréquence des attaques et l'augmentation de leur impact rendent nécessaire la mise en place de mesures de sécurité.

Pour les communes vaudoises, c'est un point essentiel dans le maintien de la confiance entre les institutions publiques et la population qui font le succès de notre système étatique suisse.

Ce travail de master a permis d'analyser comment les communes vaudoises gèrent la thématique de la cybersécurité. Dans notre introduction, nous partions de l'hypothèse que « la gestion des questions liées à l'informatique et à la cybersécurité diffère beaucoup entre ces dernières ». Cette hypothèse s'est révélée exacte

Notre première question de recherche aspirait à découvrir quels étaient les défis rencontrés par les communes dans la mise en place de mesures de cybersécurité crédibles et si la taille de la commune avait un impact. Voici ce que notre étude a permis de découvrir :

- Les difficultés budgétaires représentent un frein à la mise en place d'une stratégie crédible de cybersécurité. Les communes du canton de Vaud, dans leur grande majorité, disposent de relativement petits budgets. Ce manque de moyens implique que des choix doivent être faits et que, pour certaines communes, l'informatique, la digitalisation et la cybersécurité ne sont pas des investissements prioritaires. Certaines petites communes n'ont pas de budget dédié à l'informatique. Ce manque de moyens se reflète dans le faible pourcentage de communes mettant des ordinateurs à la disposition de leurs municipaux (32,69%). Toutefois, la problématique est reconnue. Durant les 5 dernières années, les budgets informatiques et de cybersécurité ont augmenté (69,81%).

- Dans certaines communes de petite taille, un poste de responsable informatique n'existe pas. Lorsqu'il existe, il s'agit dans la majorité des cas d'un membre de la municipalité. Une minorité de communes compte parmi ses employés des personnes disposant de compétences spécialisées en informatique. Au niveau de l'importance stratégique donnée à la digitalisation des services communaux, la majorité des communes indiquent une importance moyenne ou élevée. En ce qui concerne la problématique de la cybersécurité, les communes reconnaissent une importance stratégique importante.

- Un point intéressant soulevé par l'un des conseillers municipaux que nous avons interrogé, concerne le rapport coût/bénéfice pour la mise en place de services digitalisés dans la mesure où l'utilisation des services en ligne reste extrêmement limitée dans le cas d'une petite commune, alors que l'investissement est important. L'offre de services en ligne à la population entre les centres urbains et les petites communes diffère ainsi grandement. Cette question du rapport coût/bénéfice peut également s'appliquer à la question de l'investissement dans la cybersécurité qui peut se révéler important pour une petite commune.

- Les communes du canton de Vaud dépendent de prestataires externes pour gérer leurs infrastructures informatiques. Dans une majorité des cas, les communes stockent et

sauvegardent leurs données sur des serveurs externes, qu'il s'agisse de ceux de leurs prestataires ou de services cloud. Du fait de leurs activités, elles stockent des données personnelles et financières sur leurs résidents. En raison de la doctrine vaudoise de libre marché, chaque commune négocie de manière indépendante les conditions et les services fournis. Cette méthode a des avantages : en cas d'attaque réussie contre un prestataire, le nombre de communes impactées est limité car le système est décentralisé. Cela a également pour avantage de pousser les prestataires à proposer des conditions intéressantes afin d'être compétitifs sur le marché. Il existe toutefois des inconvénients : il n'existe pas aujourd'hui de liste d'exigences en termes de cybersécurité équivalentes pour toutes les communes. Il en résulte que le niveau de protection peut être très différent selon le prestataire et le contrat conclu avec la commune. Cela peut poser des problèmes au niveau du respect des prescriptions de la loi vaudoise sur la protection des données qui implique que celles-ci soient stockées dans des pays dont la législation est compatible avec le niveau de protection suisse. Le niveau de service peut également être impacté par ces différences relatives aux exigences. Alors qu'une commune pourra contacter son prestataire 24h/24 7j/7 en cas de problème, une autre ne le pourra pas. Un autre inconvénient relevé dans les remarques concerne le faible pouvoir de négociation des petites communes pour obtenir des conditions intéressantes auprès de leurs prestataires externes.

- Les communes restent indépendantes dans la mise en place de leurs procédures internes de gestion de la cybersécurité et de réponse en cas d'incident. Alors que certaines semblent s'être préparées à l'éventualité d'une attaque, d'autres n'ont pas de procédures en place. Les autorités cantonales souhaitent garder le contrôle en cas de problème, car elles estiment que la crise ne peut pas être gérée par les seules autorités communales.et que la gestion de crise nécessite des compétences spécifiques et ne peut pas s'improviser. Une question plusieurs fois abordée, que ce soit par l'Union des Communes Vaudoises (UCV) ou par les autorités cantonales, concerne la gestion des ressources en cas d'incident et le développement d'un SOC (Security Operation Center) capable à la fois de répondre aux demandes des communes tout en assurant les besoins des systèmes de l'administration cantonale. Cette question est politique, car il y a des décisions en lien avec le financement de cette infrastructure.

- La formation semble être un point très important pour les communes. Parmi les communes ayant répondu, elles sont 2/3 à avoir offert des formations à leurs collaborateurs. Il est important de noter que les élus devraient également recevoir une telle formation, afin qu'ils ne soient pas victimes de tentatives de phishing ou autre.

- Le système vaudois reste encore très cloisonné et les communes travaillent chacune de leur côté, ne partageant que peu les unes avec les autres. Cela a pour conséquence que les municipaux peuvent se retrouver seuls lorsqu'ils sont confrontés aux questions de cybersécurité et ne savent pas exactement vers qui se tourner. Les communes doivent, chacune de leur côté, créer des règles et des procédures.

- Les communes, dans leurs remarques, appellent à des mesures de centralisation pour certaines compétences et souhaitent mieux partager les bonnes pratiques entre elles. Du fait de la similitude des processus et des données gérées, elles souhaitent pouvoir bénéficier d'un guide de classification de la confidentialité des données et des mesures nécessaires à mettre en place pour les protéger.

- Les grandes communes ont créé une association où les responsables informatiques se rencontrent régulièrement pour traiter des sujets en lien avec l'informatique et la

cybersécurité (l'AVRIC) à laquelle l'ensemble des responsables de petites communes peuvent envoyer un représentant.

Notre seconde question de recherche s'intéressait aux bonnes pratiques que les communes peuvent mettre en place pour une stratégie de cybersécurité crédible. Notre section de recommandations a tenté d'y répondre sur la base d'une analyse de risque générale. Voici quelques points à retenir :

- **Nommez une personne responsable de l'informatique :** la création de cette position au sein de l'administration communale permet de s'assurer qu'une personne gère de manière active les questions en lien avec l'informatique, qu'elle est la personne de référence pour les prestataires externes et qu'elle peut recevoir des formations en cas de besoin.
- **Créez un budget dédié à cette thématique :** la création d'un budget dédié à l'informatique permet de garder un œil sur les dépenses liées à cette thématique et la place comme un enjeu stratégique au niveau de l'administration communale.
- **Définissez vos processus clés :** il est important de définir quels sont les processus et les données de votre administration communale que vous voulez protéger en priorité.
- **Faites appel à un prestataire indépendant pour la réalisation d'un audit :** la cybersécurité ne s'improvise pas. L'idéal est de faire appel à un prestataire indépendant pour la réalisation d'un audit de l'état actuel de la cybersécurité de la commune.
- **Intégrez la cybersécurité dans votre analyse de risque :** la cybersécurité doit être comprise dans votre analyse de risque.
- **Sélectionnez vos mesures de protection en fonction de votre analyse de risque :** il existe des centaines de mesures de protection. Faites votre sélection selon vos priorités identifiées dans votre analyse de risque et votre définition des processus clés.
- **Formation avant tout :** la formation des collaborateurs et des élus est centrale dans la prévention des évènements de cybersécurité.
- **Soyez proactifs dans la création de collaborations :** les collaborations et les partages intercommunaux et avec le canton sont de plus en plus demandés par les responsables communaux. Soyez proactifs !

Il reste beaucoup de travail pour faire en sorte que les communes du canton de Vaud soient en mesure d'atteindre un niveau de maturité élevé en matière de cybersécurité. Nous espérons toutefois que notre étude pourra être une pierre à l'édifice de cette thématique et qu'elle puisse servir de référence pour de futurs projets, que ce soit sur le plan académique ou politique.