Secrétariat du Grand Conseil **M**

Proposition présentée par les députés :
Grégoire Carasso, Léna Strasser, Alberto Velasco,

Date de dépôt : 6 mars 2023

Proposition de motion

Pour améliorer la sécurité numérique des personnes face à la cybercriminalité

Le GRAND CONSEIL de la République et canton de Genève
considérant :

– Les développements rapides des technologies de l'information, de la communication et de l'intelligence artificielle, et les risques croissants que celles-ci font peser sur la sécurité des personnes physiques et morales, mais aussi sur le fonctionnement des collectivités publiques ;
– L'augmentation massive des cas de cyberattaques au cours des dernières années dans la plupart des pays industrialisés, y compris en Suisse ;
– La complexité de la lutte contre ce type nouveau de menaces, notamment en lien avec leur caractère protéiforme et les très nombreuses cibles potentielles ;
– La relative faiblesse des outils disponibles en Suisse et à Genève en particulier pour prévenir et lutter contre ce nouveau type de criminalité ;
– Le désarroi dans lequel peuvent se trouver, par voie de conséquence, les victimes de cyberattaques, qui n'osent parfois même pas dénoncer ces actes ;
– Le vote du Grand Conseil en septembre 2022 en faveur de l'introduction d'un nouveau droit fondamental relatif à l'intégrité numérique dans la Constitution genevoise ;

invite le Conseil d'Etat à

- Augmenter les ressources publiques dédiées à la prévention et la lutte en matière de cybercriminalité afin d'améliorer à Genève la sécurité numérique des personnes physiques et morales ;
- Encourager les victimes à dénoncer tout cyberincident, quel qu'en soit le degré de gravité, et ce notamment au moyen de larges campagnes d'information ;
- Renforcer la disponibilité et la visibilité des prestations offertes aux personnes physiques (guichet du Centre national pour la cybersécurité, ligne téléphonique et accueil dans les postes de police) ;
- Etudier la création d'une offre publique-privée de prestations de cybersécurité mise à la disposition spécifique des PME ;
- Soutenir la formation dans le domaine de la sécurité numérique et la protection de la personnalité dans le champ numérique, de la prévention à l'école primaire jusqu'aux filières techniques et académiques les plus pointues ;
- Rassembler, sur le modèle de Zurich, les compétences les plus pointues sur le front de la lutte contre la cybercriminalité (procureurs, gendarmes, inspecteurs, informaticiens, praticiens, académiques, etc.) afin, en particulier, de favoriser les échanges d'informations et approches interdisciplinaires ;
- Créer une délégation à la sécurité numérique rassemblant les autorités exécutives genevoises ;
- Veiller à ce que les communes, les villes, les structures privées et la population soient adéquatement intégrées à la stratégie nationale de protection contre les cyberrisques ;
- Favoriser l'émergence d'un écosystème interdisciplinaire de recherche et d'innovation permettant de mettre en commun et développer les solutions et talents à même de contrer les modèles criminels ;
- Développer et encourager les initiatives visant à renforcer les partenariats, collaborations et échanges d'informations (du local au global, entre acteurs publics comme privés) tels que le CyberPeace Institute, la Trust Valley, la Swiss Cyber-Security Association ou CH++ ;
- Travailler à la création d'une agence européenne et/ou internationale basée à Genève et visant à promouvoir la paix et la sécurité numériques.

EXPOSÉ DES MOTIFS

Mesdames et
Messieurs les députés,

Les développements rapides des technologies de l'information, de la communication et de l'intelligence artificielle (internet, réseaux sociaux, télétravail, visioconférence, domotique, ChatGPT, metavers, etc.) ouvrent de formidables opportunités sociales et économiques. Ils représentent aussi de vertigineux risques pour la sécurité des personnes (physiques et morales) et des collectivités publiques. Cette transformation numérique de notre société doit être accompagnée par le déploiement de ressources en capacité de répondre à l'explosion des activités illégales menaçant l'intégrité, la confidentialité et la disponibilité des systèmes informatiques et des données.

La cybercriminalité est un phénomène complexe, international, aux facettes multiples, depuis les crimes dont la prévalence, l'impact et l'échelle sont accélérés par des outils informatiques (pédopornographie, ou désinformation par exemple) jusqu'aux crimes où l'informatique est la source et la cible des cyberattaques (rançongiciel ou cyber espionnage par exemple). L'ingéniosité et l'impunité des cybercriminels s'appuient sur un écosystème criminel international extrêmement agile et coopératif.

En décembre dernier, le directeur de Zurich Insurance, l'une des plus grandes sociétés d'assurance en Europe, déclarait au Financial Times que les cyberattaques, plus que les catastrophes naturelles, pourraient devenir « inassurables ».[1] Selon Interpol, la cybercriminalité est devenue une menace majeure.[2] Le montant des pertes estimé en 2021 rien qu'aux Etats-Unis est de $6.9 milliards.[3] Or la Suisse est encore mal outillée pour prévenir et gérer ces nouvelles formes de menaces. Le Global Cybersecurity Index, publié par l'Union internationale des télécommunications, classe notre pays à la 42e place, derrière Chypre et devant le Ghana.[4]

[1] « The chief executive of one of Europe's biggest insurance companies has warned that cyber attacks, rather than natural catastrophes, will become "uninsurable" as the disruption from hacks continues to grow » (FT, 26 décembre 2022 « Cyber attacks set to become 'uninsurable', says Zurich chief »).
[2] Le Temps, 25 octobre 2022, p. 15
[3] FBI, IC3, Internet Crime Report, 2021
[4] International Telecommunication Union, Global Cybersecurity Index 2020, p. 30

Au niveau de la Confédération, 30'351 infractions cybercriminelles ont été dénombrées selon l'Office fédéral de la statistique en 2021.[5] En termes de cyberagressions, on estime qu'une attaque a lieu toutes les 11 secondes en Suisse (env. 2,9 millions/an).[6] Des sources évoquent des taux de croissance à trois chiffres, faisant écho à la numérisation de pans toujours plus nombreux de la société et donc à l'augmentation de la surface d'attaque disponible.[7] Ainsi, les risques concernent le fonctionnement et les données non seulement des infrastructures publiques (dans les domaines de la santé, de l'impôt, de l'énergie, des transports, de la sécurité, etc.) mais aussi des structures privées (grandes ou petites) et des personnes physiques (toutes les catégories d'âges sont concernées).

En regard de ce très large éventail de cibles et de victimes potentielles, les cybermenaces sont elles aussi d'une grande diversité : rançongiciels, phishing-vishing-smishing, fraude à l'investissement, arnaque au président, fake sextortion, courriels de menace des autorités, escroquerie au chèque, cybersquatting, piratage sur les réseaux sociaux, pièges d'abonnement aux paquets, etc.[8]

A l'échelle suisse, le Centre national pour la cybersécurité (NCSC)[9] a réalisé une évaluation de la stratégie nationale de protection de la Suisse contre les cyberrisques.[10] Dans ses recommandations, il invite notamment à augmenter les ressources et à associer plus étroitement les PME, les cantons, les villes, les communes et la population à la gouvernance et mise en œuvre de cette stratégie.[11] Sur le terrain des enquêtes, ainsi que le rappelle Yves Nicolet, procureur fédéral chargé de la cybercriminalité, la « majeure partie des enquêtes liées à la cybercriminalité sont menées par les polices et les procureurs des cantons »[12]. Selon la même source, la référence en Suisse se trouve depuis 2013 dans le canton de Zurich avec la création d'un centre de

[5] OFS, Statistique policière de la criminalité (SPC) 2021
[6] Tribune de Genève, 8 juillet 2022, p. 5
[7] Le Temps, 15 décembre 2022, p. 11
[8] Cette liste exemplative a été établie sur la base de l'inventaire des cybermenaces du Centre national pour la cybersécurité (NCSC, https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/aktuelle-zahlen.html 21 février 2023).
[9] Le NCSC deviendra un office fédéral en mars 2023 et disposera d'environ 70 postes de travail (Le Temps, 5 décembre 2022, p. 9). Relevons que du côté de l'armée, le Parlement a décidé de doter le commandement cyber de 6000 et 7000 militaires à l'horizon 2030 (Tribune de Genève, 14-15 avril 2022, p. 17).
[10] NCSC, econcept AG, « Évaluation de l'efficacité de la stratégie nationale de protection de la Suisse contre les cyberrisques pour les années 2018 à 2022 », Rapport final, 28 mars 2022.
[11] Voir pp. 42, 44-45 et 47.
[12] Le Temps, 26 novembre 2022, p. 3

compétence rassemblant toutes les expertises pour faire face à cette forme spécifique de criminalité.

A Genève, dans le cadre d'un sondage mené par l'institut Edgelands en 2022, 75% des personnes interrogées déclaraient se sentir en situation d'insécurité numérique et attendre des autorités une meilleure protection face aux dangers en ligne.[13]

Du côté des collectivités publiques, et à la différence d'autres régions, 44 communes disposent de ressources mutualisées (via le Service intercommunal d'informatique – SIACG) tandis que la Ville et l'Etat de Genève gèrent leur système d'information de manière autonome. Pour 2021, l'Office cantonal des systèmes d'information et du numérique (OCSIN) indique avoir repéré 42'865 alertes, dont 104 ont nécessité des interventions spécifiques.[14]

Au sein de la police genevoise, la Brigade de cyberenquête, créée en 2021, compte 18 agents spécialisés et a traité en 2021 2'600 affaires.[15] Son capitaine, Patrick Ghion, considère que les PME sont parmi les cibles les plus vulnérables « car elles rapportent davantage que des individus isolés et sont généralement moins bien protégées que les grosses entreprises ».[16] L'enquête conjoncturelle 2022 de la Chambre de commerce, d'industrie et des services de Genève montre d'ailleurs que la cybersécurité est en tête des préoccupations des entreprises.[17]

Enfin, sur le plan légal, le Grand Conseil a adopté en septembre 2022 la loi constitutionnelle intitulée « Pour une protection forte de l'individu dans l'espace numérique » (L12945). Prochainement soumise à l'approbation du peuple, cette loi introduit dans notre Constitution un nouveau droit fondamental relatif à l'intégrité numérique, qui inclut notamment « le droit d'être protégé contre le traitement abusif des données liées à sa vie numérique » et « le droit à la sécurité dans l'espace numérique » (article 21A, alinéa 2).

[13] Le Temps, 17 décembre 2022, p. 15
[14] Tribune de Genève, 27 juin 2022, p. 7. Le budget de l'OCSIN dédié à la sécurité est de CHF 9 millions par an et compte une quinzaine de spécialistes.
[15] Tribune de Genève, 8 juillet 2022, p. 5. Cette brigade collabore avec deux autres services de police : la Brigade de criminalité informatique (19 personnes) et celle des renseignements criminels (3 personnes). Notons encore que la police genevoise héberge le Centre régional de compétence cyber pour la Suisse occidentale (RC3) au sein duquel ces trois groupes œuvrent en fonction de leur mission, respectivement investigation, forensique et analyse (Le Temps, 29 juillet 2022, p. 9).
[16] Ibidem
[17] CCIG info, n°6, juin 2022, p. 5

Dans cette perspective, cette motion invite le Conseil d'Etat à augmenter les ressources publiques dédiées à la prévention et la lutte en matière de cybercriminalité afin d'améliorer à Genève la sécurité numérique des personnes physiques et morales ; ce point est le cœur de cet objet dans la mesure où les autres invites en découlent. Précisons qu'il est bien question d'augmenter les moyens publics et non de les réallouer en affaiblissant d'autres prestations.

La motion invite par ailleurs à encourager les victimes à dénoncer tout cyberincident, quel qu'en soit le degré de gravité, et ce notamment au moyen de larges campagnes d'information ; ces démarches permettent non seulement d'apporter du soutien aux victimes mais aussi de partager de l'information et donc d'améliorer la prévention et les réponses apportées aux attaques. Afin de faciliter ces démarches, nous souhaitons renforcer la disponibilité et la visibilité des prestations offertes aux personnes physiques (guichet du Centre national pour la cybersécurité, ligne téléphonique et accueil dans les postes de police). Le texte propose également la création d'une offre publique-privée de prestations de cybersécurité mise à la disposition spécifique des PME. Plus largement et dans une perspective de long terme, la motion invite à soutenir la formation dans le domaine de la sécurité numérique et la protection de la personnalité dans le champ numérique, de la prévention à l'école primaire jusqu'aux filières techniques et académiques les plus pointues.

Sur le plan organisationnel et institutionnel, cette motion ouvre trois axes : en premier lieu rassembler, sur le modèle de Zurich, les compétences les plus pointues sur le front de la lutte contre la cybercriminalité (procureurs, gendarmes, inspecteurs, informaticiens, praticiens, académiques, etc.) afin de favoriser les échanges d'informations et approches interdisciplinaires ; en deuxième lieu, sur le plan politique, créer une délégation à la sécurité numérique rassemblant les autorités exécutives genevoises à même de donner des impulsions et d'offrir une gouvernance partagée. En troisième lieu, ainsi que le recommande le rapport d'évaluation de l'efficacité de la stratégie nationale de protection de la Suisse contre les cyberrisques cité plus haut, nous souhaitons que les communes, les villes, les structures privées et la population soient adéquatement intégrées à cette stratégie.

Enfin, à une échelle plus large et tout en considérant la valeur ajoutée que pourrait représenter Genève en termes de gouvernance, de diplomatie scientifique et de sécurité collective, la motion invite à favoriser l'émergence d'un écosystème interdisciplinaire de recherche et d'innovation permettant de mettre en commun et développer les solutions et talents à même de contrer les modèles criminels. Elle propose également de développer et d'encourager les

initiatives visant à renforcer les partenariats, collaborations et échanges d'informations (du local au global, entre acteurs publics comme privés) tels que le CyberPeace Institute, la Trust Valley, la Swiss Cyber-Security Association ou CH++. Enfin, le texte invite le Conseil d'Etat à travailler sur le projet de création d'une agence européenne et/ou internationale basée à Genève et visant à promouvoir la paix et la sécurité numériques.

L'approche large et englobante de cette motion est doublée d'un projet de loi modifiant de manière ciblée la loi sur la police. Ces deux démarches sont complémentaires et visent le même but : renforcer la sécurité numérique des personnes (physiques et morales) à Genève.

Au vu de ce qui précède, nous vous remercions Mesdames les députées, Messieurs les députés, de réserver un bon accueil à la présente proposition de motion.