

«Avec le développement de l'IA, chacun peut devenir un cybercriminel»

Genève, ville-monde La cybersécurité pose plusieurs défis, sur le plan local comme international. Carole-Anne Kast et Stéphane Duguin les analysent et présentent une collaboration inédite.

Sophie Davaris et Marc Bretton

En partenariat avec le Club diplomatique qui fête son 50^e anniversaire, la «Tribune de Genève» propose des dialogues entre des figures de la vie locale et des acteurs de notre cité internationale. Le troisième volet de cette série est consacré à la sécurité informatique.

La conseillère d'État responsable de la police et du numérique Carole-Anne Kast et Stéphane Duguin, directeur exécutif du CyberPeace Institute affrontent les défis croissants liés à la cybersécurité. Indépendance, fiabilité des données, pérennité: des problématiques extrêmement locales et globales à la fois.

Quels défis affrontez-vous en matière de cybersécurité?

Carole-Anne Kast (C.-A.K.): À l'État, la sécurité informatique consiste d'abord à lutter contre la cybercriminalité. Cette mission, confiée à la police, recouvre deux volets. Il s'agit d'une part de traquer le vol de données contre rançon (*ransomware*), le chantage – souvent à caractère sexuel

(*sextorsion*) –, l'envoi de fausses factures, les amendes via SMS, WhatsApp ou Signal, et la pédopornographie. Le deuxième volet consiste à lutter contre les professionnels du crime qui recrutent, via TikTok par exemple, des petites mains afin de commettre des délits. Ou qui incitent de jeunes mineurs à se prostituer sans qu'elles aient conscience d'être exploitées par des proxénètes.

L'autre dimension de la sécurité informatique, à l'État, est la cyberdéfense, soit la protection de l'activité de l'État et des données que les citoyens lui confient. *Stéphane Duguin (S.D.):* La mission du CyberPeace Institute, fondation opérationnelle genevoise de droit public à but non lucratif, est de protéger les ONG dans le cyberspace. Nous aidons 650 ONG – une centaine en Suisse, dont 71 à Genève – à se protéger en matière de cybersécurité.

Comment aidez-vous les ONG?

S.D.: Les instruments et les instructions pour se protéger se trouvent sur internet. Tout est gratuit, en ligne. Mais cela ne fonctionne pas, car pour les in-

dividus comme pour les entreprises, la sécurité n'est pas un réflexe premier. Ils sont occupés à mener leur vie et leurs activités. C'est compréhensible.

Pourtant, dès qu'on choisit un moteur de recherche, une base de données, des programmes, dès qu'on répond à des formulaires en ligne, on génère des données. La question de la cybersécurité se pose alors pour tous, que l'on soit un individu ou une ONG.

Le CyberPeace Institute offre aux ONG une main-d'œuvre formée afin de sécuriser leurs données, analyser les problèmes, proposer des solutions. C'est une expérience unique au monde, pratiquement un label genevois, exportable, qui s'effectue par le biais d'un partenariat public-privé. Des entreprises (transport, technologie, cybersécurité, banques, assurances) nous mettent à disposition environ 1500 de leurs professionnels, volontaires.

Quels intérêts ont ces employés et ces entreprises à vous aider dans votre travail?

S.D.: Les grandes entreprises veulent attirer et retenir des talents. Or, chez les employés,

l'envie d'aider et de sauver le monde est beaucoup plus répandue qu'on ne le croit. Pour les sociétés, c'est un argument et une manière de se distinguer positivement par rapport à la concurrence et un moyen concret de remplir leurs objectifs en termes de responsabilité sociale. Cette aide n'est pas un marché volé à des entreprises. Le plus souvent, les ONG n'ont pas les moyens d'investir dans la sécurité informatique.

Dans quelle mesure le Canton est-il visé par des attaques informatiques?

C.-A.K.: Les chiffres sont étourdissants. En 2025, nous avons relevé 350 milliards d'événements (+25% en un an, car ils sont mieux détectés), soit 11'000 par seconde. Ils ont généré 36'885 alertes, dont 519 ont été considérées comme des incidents de sécurité (+38%). Cela signifie 1,4 incident par jour.

En tête des administrations attaquées: le pouvoir judiciaire, l'administration fiscale ou encore la Fondation des parkings. On recense plusieurs types d'attaque: le *phishing* (vol de données, *ransomware*), les



La conseillère d'État Carole-Anne Kast et le directeur exécutif du Cyberpeace institute Stéphane Duguin évoquent les défis que pose la sécurité informatique. Laurent Guriaud

attaques d'approvisionnement (utilisation des données d'un tiers pour voler vos données), des vols (fausses amendes).

Quels sont les moyens consacrés à la protection numérique?

C.-A.K.: L'Office cantonal des systèmes d'information emploie plus de 20 personnes à la protection numérique. Le budget s'élève à 3 millions de francs de fonctionnement et à un peu moins de 2 millions par an d'investissement. Par ailleurs, les différents départements emploient 11 répondants responsables de la sécurité informatique. Au sein de la police, trois entités s'occupent de cybercriminalité. *S.D.:* Pour les États, les dégâts peuvent être importants. En 2022, l'administration du Costa Rica a été mise à terre par une vague de rançongiciels. C'est la première fois qu'on qualifiait une cyberattaque de terrorisme.

Les ONG subissent-elles des attaques d'une même ampleur?

S.D.: Bien sûr. Les ONG sont le deuxième secteur le plus attaqué, après le secteur financier. Elles sont des victimes comme les PME. Les sommes en jeu sont

gigantesques; les montants volés sont parfois faibles par victime, mais très nombreux. Du coup, la fraude en ligne rapporte plus que le trafic de drogue! Comme pour les attaques visant des personnes, la cybercriminalité contre les ONG s'opère en cascade. Et le phénomène s'accélère. Avec le développement de l'intelligence artificielle, chacun peut devenir un cybercriminel. On observe aussi des attaques ciblées liées à des conflits, comme la guerre en Ukraine. Mais ce qui est important, ce n'est pas tant le nombre d'attaques sur les ONG que leur impact sur le terrain et le temps nécessaire pour fonctionner à nouveau. Ce qui frappe aussi, c'est le dommage psychologique: une victime de cybercriminalité a honte de s'être fait avoir.

L'État et le Cyberpeace Institute ont-ils des projets communs en matière de cyberrésilience?

C.-A.K.: Depuis 2024, le Canton et la Ville ont mandaté le CyberPeace Institute pour renforcer la cyberrésilience des habitantes et habitants, par différentes actions. *S.D.:* Le projet Éclaire a d'abord consisté à aller à la rencontre de Monsieur et Madame Tout-le-

«C'est un enjeu important. Les réseaux ne sont pas des lieux bienveillants, mais des espaces de non-droit sur lesquels traînent des prédateurs, des voleurs, des criminels.»

Carole-Anne Kast

Conseillère d'État responsable de la police et du numérique.

Monde. Il s'est agi, par exemple, d'apprendre à des seniors à envoyer des SMS, d'aider des jeunes à monter une entreprise en connaissant les risques de l'IA, à donner des formations aux associations.

Le deuxième volet vise à créer une cartographie de l'ensemble des offres de résilience numérique à Genève, pour mieux orienter

les gens vers des associations de terrain comme Tech Against Violence, OSEO ou Action Innocence. Ou faciliter des coopérations interassociatives. Par exemple, si l'Avivo met en place une formation, elle pourra voir ce que fait le Mouvement des aînés. L'intérêt est double: le citoyen accède à une formation, et les associations acquièrent une vision globale de ce qui existe en matière de sécurité informatique.

Genève peut-elle développer une expertise pour assurer sa place dans le monde international en plein bouleversement?

S.D.: L'ancien modèle ne reviendra pas. Les ONG doivent fonctionner en synergie. Nous pensons que ce modèle Éclaire, développé à Genève, pourra trouver des financements et être transposé au niveau international. Il y a effectivement à Genève, et plus largement sur l'arc lémanique, un écosystème très particulier lié à la cyberéconomie, à la société civile, aux entreprises, aux hautes écoles, au projet de Trust Valley qui offre des perspectives très intéressantes autour de la notion de confiance numérique. *C.-A.K.:* C'est un enjeu important.

Les réseaux ne sont pas des lieux bienveillants, mais des espaces de non-droit sur lesquels traînent des prédateurs, des voleurs, des criminels. Si la fracture numérique liée à l'âge se réduit, elle laisse la place à une vulnérabilité qui concerne chacun d'entre nous. Les réseaux sociaux sont des espaces à civiliser, à réguler. Cela passe par l'abolition de l'anonymat. Et au niveau collectif par le développement de lieux de stockage des données, des clouds souverains, publics et bien sécurisés, comme ce que développe la Suisse et les cantons dans le Swiss Government Cloud.

Des solutions souveraines sont-elles possibles?

S.D.: La fin de l'anonymat? Naturellement. La fin du secret bancaire était vu comme une chose impossible, et puis c'est devenu parfaitement possible. Pour le Cloud, cela s'impose: il faut agir. L'attentisme ne paye pas. Il faut élaborer une stratégie consciente permettant de savoir ce que l'on veut. Au niveau des États et des individus, il faut mettre en place un système d'autodéfense intellectuel et se rappeler que les réseaux ne veulent pas notre bien.