Ville de Genève
Conseil municipal

M-772 A

9 novembre 2015

Rapport de la commission de l'informatique et de la communication chargée d'examiner la motion du 20 février 2008 de MM. Vincent Maitre, Alain de Kalbermatten, Jean-Charles Lathion, Robert Pattaroni, Mmes Anne Carron-Cescato, Marie Chappuis, Nelly Hartlieb, Alexandra Rys, Odette Saez, Florence Kraft-Babel, MM. Alexandre Chevalier, Jean Sanchez et Alexis Barbey: «Sécurité informatique: connectons-nous à la réalité!»

Rapport de M. Pascal Rubeli.

La motion M-772 a été renvoyée à la commission de l'informatique et de la communication lors de la séance plénière du 22 septembre 2008. L'objet a été traité lors des séances des 27 octobre, 24 novembre 2008, 5 et 19 janvier et 2 et 9 mars 2009 sous la présidence de M. Jean Sanchez. Les notes de séances ont été prises par M. Daniel Zaugg, que nous remercions de son travail.

Rappel de la motion

Considérant:

- que le piratage informatique représente la deuxième économie parallèle mondiale après le trafic d'armes international;
- que le piratage informatique, représentant 200 milliards de dollars en 2006, est devenu plus lucratif que le trafic mondial de stupéfiants (chiffre officiel du FBI);
- que la cybercriminalité a changé de visage et qu'elle est déformais structurée et organisée en réseau de malfaiteurs, à des fins essentiellement lucratives;
- que le piratage informatique constitue la forme de menace terroriste la plus importante du XXIe siècle;
- que les entreprises spécialisées dans le piratage éthique *(ethical hacking)*, soit le piratage sur mandat afin de tester la sécurité du système informatique d'un particulier, connaissent un taux de réussite de 100% en quelques heures;
- qu'il en coûterait, selon une étude de l'Ecole polytechnique fédérale de Zurich, quelque 5,83 milliards de francs par semaine pour l'économie suisse en cas d'attaque sur toutes les grandes entreprises;
- que plus de 50% des entreprises françaises ont été piratées, bien que ce pays soit plus avancé que la Suisse en matière de sécurité informatique;
- que Swisscom a déjà été victime d'une attaque informatique le 7 janvier 2008;
- que certaines banques, en Suisse, ont également été victimes d'attaques engendrant des pertes de plusieurs dizaines de millions de francs au cours des dernières années;

– que la plupart des banques privées à Genève ont dû faire tester la sécurité de leur système informatique par des entreprises indépendantes spécialement qualifiées;
– que la plupart des collectivités sont peu conscientes du danger et n'ont, en conséquence, encore rien entrepris pour sécuriser leur système informatique et protéger leurs données de façon efficace;
– qu'il en découle une violation de la Constitution fédérale, article 13, et de la loi fédérale sur la protection des données (LPD), articles 1 et 2 et article 7, alinéa 1 notamment,

le Conseil municipal demande au Conseil administratif de mandater une entité indépendante et privée, reconnue par l'Etat et, en conséquence, autorisée à traiter des données confidentielles, afin de détecter les failles, évaluer les risques et protéger le patrimoine informationnel ainsi que le réseau informatique de l'administration municipale de la Ville de Genève.

Séance du 27 octobre 2008

Audition des motionnaires

Le président donne la parole à M. Vincent Maitre qui s'exprime au nom des motionnaires.

Il explique que, si la liste des considérants peut sembler alarmiste, des faits récents démontrent malheureusement qu'elle est totalement d'actualité. Il constate que la Ville de Genève n'a pas encore été touchée par ce problème mais qu'en revanche ce n'est pas le cas de l'Etat et d'un certain nombre d'entreprises privées (Kudelski) ou publiques telles que Swisscom, que le piratage informatique, selon le FBI, génère des revenus de l'ordre de 200 milliards par année et que c'est désormais la deuxième économie souterraine après le trafic des stupéfiants. On voit donc bien que ce problème peut toucher à la fois les grosses entreprises, mais aussi des particuliers. Il précise qu'il y a également un piratage qui alimente des réseaux terroristes. Il indique, à cet égard, que l'entreprise Skyguide a pu à titre expérimental être infiltrée et que donc le problème est très sérieux. Il ajoute que les entreprises spécialisées dans le piratage éthique *(ethical hacking)*, soit le piratage sur mandat afin de tester la sécurité d'un système informatique d'un particulier ou d'une entreprise, connaissent un taux de réussite de 100% en quelques heures. Il conclut en expliquant que le piratage informatique est par définition toujours en avance sur les choses et que les informaticiens de la DSIC, compte tenu de leur formation et de leur cahier des charges, n'ont probablement pas toutes les compétences requises pour résister à des groupes bien organisés. Il faut donc faire appel à des entreprises spécialisées dans le but de lutter contre ce piratage. Il propose donc concrètement de mandater un établissement privé afin d'auditer la DSIC.

M. Sanchez, motionnaire confirme qu'il serait très difficile pour la DSIC de s'auditer elle-même car ses informaticiens auraient de la peine à prendre le recul nécessaire requis pour entreprendre une telle démarche. Il faut donc recourir à un organisme externe.

M. Maitre stipule que la protection informatique fait l'objet d'une obligation légale figurant à l'article 13 de la loi fédérale sur la protection des données (LPD) dans ses articles 1, 2 et 7, alinéa 1 notamment.

Un commissaire aimerait connaître ces «hackers» et comprendre comment ils fonctionnent? Il souhaiterait également savoir comment de pareils fonds criminels à hauteur de 200 milliards peuvent être générés ou perçus. S'agit-il de monnaie numéraire (billets de banque et pièces) ou scripturale (comptes bancaires ou argent électronique)?

M. Maitre répond que les interventions électroniques des «hackers» portent sur des avoirs en compte qui peuvent être donc matérialisés sous forme de monnaie numéraire, c'est-à-dire de billets de banque. Différentes techniques sont utilisées parmi lesquelles l'introduction de virus via des spams donnant accès au logiciel des entreprises. Ce processus est actuellement exponentiel. M. Sanchez relève, afin d'illustrer l'origine du montant de 200 milliards, la multiplication des cartes de crédit et l'augmentation d'une certaine criminalité liée à leur utilisation. Il ajoute, pour mieux définir le profil du «hacker», qu'il y a des magazines et des sites internet qui proposent des méthodes de formation et qu'il y a même chaque année à Las Vegas un concours amateur qui est organisé dans ce but afin d'obtenir des places inté- ressantes y compris au sein du FBI et de la CIA!

M. Maitre signale que nous sommes tous et toutes à notre façon des «hackers» quand nous téléchargeons illégalement des programmes ou des musiques. Dans un autre ordre, il stipule que le premier niveau de compétence de ceux qui se servent de logiciels «anti-hacking» (spywares, pare-feux, etc.) se révèle inefficace devant la duplicité de certains pirates. Les employés de banque, par exemple, n'ont pas toujours les compétences nécessaires pour faire face à une opération de piratage et constatent que leurs logiciels «anti-hacking» ne leur sont d'aucune utilité. Il convient en conséquence de faire appel à des entreprises spécialisées dans la branche afin d'être protégé.

Un commissaire demande si l'Etat a entrepris une démarche analogue? Et qu'en est-il d'autres collectivités (villes, etc.)? Enfin, à quelle entreprise M. Maitre entend-il proposer d'attribuer cet audit?

M. Maitre indique que la Ville de Zurich a mandaté une entreprise pour procéder à un audit de son système d'informatique. Il ajoute que la France est pionnière en la matière et qu'il existe dans ce pays voisin une commission infor-

matique nationale. Il conclut en indiquant que la raison sociale de l'entreprise privée à laquelle il pense a pour nom Ilion Security SA et qu'elle est située à l'avenue Cardinal-Mermillod 36. Il s'agit d'une société qui travaille, d'ores et déjà, avec de nombreuses entreprises privées ainsi qu'avec les plus hautes instances de la Confédération. La société évalue les dangers liés à l'utilisation du système d'information. Elle émet des recommandations afin de réduire ces risques.

Une commissaire se pose la question de savoir si c'est une bonne idée de mandater une entité indépendante qui pourrait de cette manière obtenir un certain nombre d'informations sur nos activités municipales et s'en servir librement après? Elle estime que la DSIC dispose, d'ores et déjà, des ressources nécessaires pour entreprendre un audit interne et détecter les failles du système utilisé.

Un commissaire propose d'auditionner des fonctionnaires dont M. Favre afin d'obtenir des éléments de réponse à ce sujet ainsi que M. Maudet. M. Maitre signale qu'à l'époque M. Muller avait proposé de mandater une société privée afin de procéder à un audit. Il pense que la société Ilion SA proposera la formule la plus adaptée au système informatique de la Ville de Genève et que le suivi de l'opération fera partie du cahier des charges proposé.

M^me^ Camporini, prenant acte du fait qu'en une demi-journée il est possible de pénétrer un système informatique, se demande par conséquent comment cela n'est pas encore arrivé en Ville de Genève. M. Maitre relève que les «hackers» normaux disposent de moyens simples et que le système informatique de la Ville de Genève est relativement complexe.

Un commissaire signale que, dans les faits, peu de collectivités politiques sont infiltrées. Il faut donc relativiser le problème en procédant à un sondage préalable auprès des sociétés spécialisées dans la branche afin de connaître les véritables risques de piratage. M. Maitre est d'accord. Il pense également que le danger est limité, mais que cela n'interdit pas de prévenir plutôt que de guérir. Il ajoute que la politique du Conseil fédéral consiste depuis peu à protéger le plus complètement possible son système informatique car les peines encourues pour les «hackers» en violation de la LPD ne sont malheureusement pas assez dissuasives. Le problème en Ville de Genève est, toutes proportions gardées, à peu près analogue à celui de la Confédération et porte essentiellement sur la confidentialité des données.

Le président remercie M. Maitre et propose d'aborder le problème des auditions. La commission accepte à l'unanimité d'entendre dans un premier temps M. Maudet accompagné de quelques collaborateurs de la DSIC et décidera ensuite des autres auditions proposées.

Séance du 24 novembre 2008

Audition de M. Pierre Maudet, conseiller administratif chargé du Département de l'environnement urbain et de la sécurité, accompagné de M. Eric Favre, directeur de la DSIC, et de M. Jean Sottas, concepteur de systèmes de communication

M. Maudet a tenu à se faire accompagner de deux de ses collaborateurs, MM. Favre et Sottas. Ce dernier a préparé une présentation pour montrer à la commission le type d'attaques dont peut être victime la DSIC. M. Maudet a bien lu les considérants de la motion qu'il trouve intéressante mais ne comprend pas très bien où certaines informations ont été «pêchées» et s'arrête sur les considérants «le piratage informatique représente la deuxième économie mondiale parallèle après le trafic d'armes international» ou bien encore «le piratage informatique représente la menace terroriste la plus importante du XXIe siècle». Il a le net sentiment qu'il s'agit là davantage de jugements de valeur plutôt que d'informations bien étayées. Il rappelle que tant son prédécesseur que lui-même ont eu à cœur de protéger les différents systèmes d'information et de communication de la Ville de Genève. Il n'a donc pas attendu cette motion pour mettre en place des audits par des entités indépendantes et privées afin de tester la sécurité desdits systèmes. Il indique, à cet effet, que la DSIC a procédé à 34 audits depuis l'année 2004 dont 27 durant ces deux dernières années. La difficulté principale réside dans le fait que les prestations de la DSIC s'adressent au public, comme dans les bibliothèques municipales. Il relève qu'il y a, sur ce plan, une certaine ambivalence, puisqu'un système sûr est par essence fermé alors même que la Ville entend l'ouvrir à un certain nombre d'usagers. Il en ressort que le talon d'Achille du fonctionnement est l'utilisateur lui-même qui peut générer par son comportement des atteintes à la sécurité informatique. C'est donc dans la multiplication des terminaux – et par conséquent des accès – que des problèmes peuvent apparaître. Il met en relief qu'on rencontre, en une année, près de 58 000 attaques informatiques à la DSIC. M. Maudet ajoute qu'il y a certains aspects de l'activité municipale qui peuvent être plus sensibles que d'autres, telles que l'état civil. Il conclut cette première présentation en énonçant que la Ville n'a donc pas attendu cette motion pour prendre un certain nombre de dispositions dans le but de protéger ses divers systèmes informatiques et rappelle qu'il propose dans le cadre du projet de budget 2009 d'augmenter cette sécurité en engageant un collaborateur supplémentaire en classe 17-19 pour pallier cela.

M. Favre précise que ce problème passe par une gestion des risques. Les questions se posent différemment selon qu'il s'agit d'une entité publique comme la Ville de Genève ou d'une banque privée. Prenant l'exemple du catalogue des bibliothèques, il précise qu'il s'agit pour la Ville de Genève de protéger son intégrité. A l'opposé, s'agissant de l'état civil, les informations transitent par des systèmes cryptés provenant de la Berne fédérale. Il y a donc en Ville une grande palette d'utilisateurs qui va de l'universitaire qui glane quelques informations dans

le site du Jardin botanique au responsable des finances qui doit protéger un certain nombre de données liées aux marchés publics. Il s'agit donc d'une pesée de risques car la DSIC fait l'objet en permanence d'un certain nombre d'attaques dont une part non négligeable sont effectuées par des robots, c'est-à-dire des logiciels qui essaient de pénétrer dans le système. Il y a en revanche des attaques ciblées mises en scène par des hackers qui peuvent produire des effets indésirables, par exemple un ralentissement du trafic des informations. Il ajoute, sur ce plan, que cela fait un certain temps qu'il n'y a plus eu d'attaques musclées des systèmes de la DSIC. Pour en revenir au problème qui préoccupe la commission, il indique que les nouvelles applications sont systématiquement testées et ne sont pas mises en ligne avant d'avoir été soumises à un audit. Il indique à ce titre que 16 nouvelles applications sont entrées en fonctionnement lors de ces deux dernières années.

M. Favre présente ensuite M. Sottas qui est concepteur de systèmes de communication. Il indique que la présentation qui va être faite porte sur le système Firewall, dispositif de sécurité qui protège la Ville contre les agressions transitant par Internet. Ce dispositif répertorie les informations que reçoit la DSIC, environ 5 millions par jour, et repère les agressions selon leur degré de dangerosité. Chaque fois qu'une connexion se produit, une trace apparaît. Elle est en vert s'il s'agit d'une connexion sans risques, donc admise, ou en rouge s'il s'agit d'un événement jugé offensif. Sur ces 5 millions de connexions par jour, un bon 10% se range dans la catégorie des agressions caractérisées. M. Favre indique à la commission que ces agressions sont bloquées automatiquement et ne nécessitent donc pas, à ce stade, d'interventions humaines. Un autre type d'attaque utilise des virus qui installent des programmes sur l'ordinateur piraté, permettant ainsi au hacker d'accéder aux informations de l'appareil et ainsi d'attaquer les réseaux connus avec un grand nombre d'ordinateurs dans le but multiplier les attaques. Le but de ce piratage est de saturer les réseaux afin de les bloquer aux autres utilisateurs. En Ville de Genève, il n'y en a plus eu depuis un certain temps et il relève que, lors de ces attaques, le système de la Ville de Genève est toujours resté en fonction. M. Favre n'est pas certain que la publicité faite autour de cette motion soit une bonne chose car il est à peu près sûr que l'attention de certains «hackers» va se porter, par voie de conséquence, davantage sur la Ville de Genève. M. Sottas précise que ces dispositifs de Firewall existent pour protéger le réseau de la Ville, son réseau public en particulier ainsi que l'infrastructure du SIS. Ces Firewall ont donc des tâches bien précises et on peut spécifier quel trafic rentre dans le système ou en sort. Cela permet de s'adapter à la demande de sécurité pour chacun de ces réseaux. Il relève, à partir d'un exemple sur l'écran de «scan de port», que le Firewall interdit là toute pénétration dans le réseau en bloquant le trafic. Ce travail se fait en permanence. La machine bloque tout par principe et n'autorise que ce qui est spécifiquement permis. La DSIC reçoit environ 5 millions de scans par jour dont 500 000 qui sont rejetés. M. Favre précise qu'il y a plusieurs réseaux en Ville de Genève: le réseau wifi, le réseau public qui est destiné aux usagers

ainsi que celui de l'administration municipale qui est, lui, beaucoup plus protégé. Il indique qu'il existe des systèmes de filtrage autres que le Firewall qui, chacun avec leurs caractéristiques propres, empêchent certaines attaques et qu'ils sont en train d'être progressivement installés.

Questions des commissaires

Une commissaire aimerait savoir comment la DSIC s'y prend pour mettre régulièrement à jour des systèmes de protection «anti-hackers» face à des pirates de plus en plus performants? M. Favre lui répond qu'il convient d'ajuster sans cesse les ripostes nécessaires en installant des logiciels de protection pour compléter le dispositif. Il ajoute que les besoins ne sont pas spécifiquement matériels, mais essentiellement humains car il convient d'engager un collaborateur ou une collaboratrice afin de pouvoir élaborer et formaliser un certain nombre de normes de sécurité.

Un commissaire souhaite que l'on prenne plus en compte la sécurité mécanique ou celle qui est liée aux télécommunications. Il ajoute que, concernant les spams, rien n'est particulièrement entrepris par la DSIC pour orienter davantage le choix des conseillères municipales et conseillers municipaux. M. Favre lui rétorque qu'il est sur ce plan impossible d'en faire plus car il y a une telle diversité de messages qu'il se peut par exemple très bien que la DSIC elle-même n'en ait pas connaissance. Ce même commissaire évoque ensuite la procédure d'engagement des collaborateurs et collaboratrices de la DSIC et demande notamment si une enquête a lieu au préalable en ce qui concerne leurs qualifications et le bien-fondé de leur motivation car il ne fait aucun doute, pour lui, qu'un passage en Ville de Genève représente pour les «hackers» une bonne carte de visite. M. Maudet relève que toute candidature fait l'objet d'une enquête préalable réalisée par un employé du Service de la sécurité et de l'espace publics qui, en l'espèce, est la personne qui s'occupe également des naturalisations. M. Favre ajoute à cela qu'une formation est distribuée aux fonctionnaires mais reconnaît qu'une certaine ambiguïté existe en ce qui concerne les conseillères municipales et conseillers municipaux en ce sens qu'il est difficile de les considérer comme des fonctionnaires et que cela peut conduire à ne pas leur octroyer le même niveau d'information que les collaborateurs et collaboratrices de l'administration de la Ville de Genève.

Une commissaire ne comprend pas l'intérêt qu'il y a pour certains «hackers» de pénétrer dans le réseau public de la Ville de Genève et demande une explication à cet égard. M. Maudet évoque tout d'abord l'aspect ludique qui prévaut dans ce milieu et indique qu'il a eu l'occasion de visiter une entreprise spécialisée dans le «hacking» éthique à Carouge. Il en ressort que l'objectif de ladite société consistait à vendre des logiciels de protection et il a pu, là, pleinement

réaliser l'addiction des jeunes employés échevelés qui y travaillaient, ressemblant à s'y méprendre à celle des personnes qui fréquentent les casinos. Au-delà de cet aspect, il y a dans les services publics des données très sensibles concernant les personnes, leur état civil, etc. et surtout il convient de relever qu'en pénétrant un réseau public, on est à même de se connecter à d'autres administrations afin d'obtenir des informations qui peuvent se monnayer ensuite sur le marché. M. Favre donne, en guise d'exemple, la possible pénétration du système financier de la Ville afin de pouvoir produire de fausses factures et toucher frauduleusement des montants indus. Il estime toutefois que les collectivités publiques ne sont pas moins bonnes que les banques mais que la gestion des risques y est différente et l'on comprendra, à cet égard, que la publication du compte à numéro d'un client important contient un risque autrement plus sensible que les données publiques d'une administration municipale. C'est la raison pour laquelle l'effectif des informaticiens dans une banque privée peut atteindre un ratio de 10 à 15%. Ceci dit, il ne faut pas négliger les attaques des systèmes de la ville, et en cela Firewall est un bon système de protection mais il est vrai que des erreurs humaines peuvent parfois conduire à des tentatives réussies de pénétration du réseau. C'est la raison pour laquelle la DSIC porte un accent très fort sur la formation de ses collaborateurs et collaboratrices.

Un commissaire relève que les conseillères municipales et conseillers municipaux reçoivent dans leur courrier un certain nombre d'objets indésirables dont certains vont dans la boîte réservée aux spams et d'autres non. Il pose donc la question de savoir si la DSIC pourrait remédier à ce problème. M. Favre indique que, pour la messagerie, la DSIC a reçu 20 millions de messages dont 18 millions qui procédaient de messages non sollicités. Il y a donc environ 90% des messages transmis à l'administration municipale qui appartiennent à cette catégorie parmi lesquels des spams, des pourriels, etc. La DSIC a donc un dispositif de tri qui précisément bloque le 90% de ces messages à l'entrée. Il y a, par conséquent, assez peu d'essais qui réussissent à passer au travers de ce dispositif. Les attaques se font souvent par vagues en modifiant un paramètre qui n'a pas encore été pris en compte par le système défensif de la DSIC.

Un commissaire demande quelle est l'appréciation par la Ville de Genève de ces risques en les comparant à celles d'autres collectivités publiques de notre pays. M. Maudet estime que l'on est dans une identification mesurée et correcte des risques en ce qui concerne les moyens affectés à la DSIC et le nombre d'audits mis en place par rapport à d'autres collectivités publiques semblables. M. Favre ajoute que le but de cette présentation était de montrer que, devant cette complexité, un seul audit confié à une entité indépendante préconisé par la motion était loin de pouvoir répondre à la question relative à la protection des systèmes informatiques de la DSIC. Ce même commissaire aimerait connaître le montant affecté par année aux audits actuels en regard avec ceux qui sont attri-

bués à d'autres municipalités de la même importance afin de se faire une idée de la pertinence de toutes ces démarches. M. Maudet qui fait le lien avec le débat budgétaire relève qu'il y a en ville une administration de 4000 collaborateurs et collaboratrices et un grand nombre d'utilisateurs qui le conduisent à mettre en place des mesures préventives. C'est la raison pour laquelle il lui semble indispensable – tout en procédant à la comparaison de ratios entre un certain nombre de collectivités publiques de notre pays – de proposer au budget un poste dédié à une mission de protection, consistant à mettre à jour un certain nombre de données technologiques, et à former les collaborateurs et collaboratrices. Il y a d'une part les montants affectés aux audits et d'autre part les coûts de la sécurité en termes de matériel.

Le président aimerait savoir si Genève est meilleure ou moins bonne que Lausanne ou Zurich. M. Favre relève que la Ville de Genève avec un taux de 1,9% de collaborateurs et collaboratrices par rapport à une moyenne suisse de 5,2% et de nombreuses administrations publiques qui tournent autour de 6,2% est, en termes de postes, sensiblement en bas de l'échelle et que c'est la raison pour laquelle elle fait appel à des mandataires externes pour auditer ses systèmes. Il en profite pour proposer que des conseillers municipaux puissent participer, une fois, à un audit afin de bien comprendre ce que cela peut représenter en terme d'heures de travail et d'investissement informatique. Il va de soi que lesdits conseillères municipales et conseillers municipaux y seraient tenus à un strict devoir de confidentialité. Le président prend cette idée au vol et la trouve intéressante.

Un commissaire demande, dans le cas où un hacker s'approprierait l'ordinateur d'un conseiller municipal, si le piratage des systèmes de la Ville en serait plus facile pour lui. M. Favre lui rétorque que la DSIC prend quelques cautèles à cet égard et qu'il est difficile d'entrer dans les systèmes de la Ville sans disposer d'un mot de passe sauf si ledit mot de passe a été stocké quelque part dans la mémoire de l'ordinateur. Le risque évident serait que ce hacker usurpât l'identité électronique d'un élu, ce qui pourrait lui ouvrir certaines portes du réseau. Il s'agit là davantage de risques personnels qui peuvent conduire à l'appropriation d'un compte bancaire, ou à d'autres situations analogues.

M. Maudet ne comprend pas très bien le contenu de l'invite qui parle «d'une entité indépendante et privée reconnue par l'Etat». Il n'a pas connaissance du fait que l'Etat reconnaîtrait dans ce domaine des entreprises indépendantes et privées. Un motionnaire explique qu'il s'agit là des mandataires reconnus par l'Etat et le Centre des technologies de l'informatique (CTI) en particulier. M. Maudet ne considère pas que CTI représente un label de qualité et pour tout dire il a eu même l'impression que la DSIC avait dans moult situations une bonne longueur d'avance sur l'Etat. Il considère donc que sur ce plan-là l'invite de la motion est d'ores et déjà pleinement réalisée.

Une commissaire en revient à ce qui avait été dit par M. Maitre qui avait énoncé lors de son audition que les attaques s'étaient intensifiées ces derniers mois, et demande à M. Favre si c'est effectivement le cas. M. Favre confirme cette assertion en indiquant que de nombreux spams vont être en particulier envoyés durant les fêtes qui, à coup sûr, vont contenir des virus et qu'il faudra être très prudent à cet égard. Il tient cependant à rassurer la commission en relevant que les systèmes de protection mis en place par la Ville sont relativement sûrs.

Un commissaire fait tout d'abord une remarque: il a l'impression que les constats qui sont faits dans la motion sont liés au monde économique et aux grandes entreprises en général et qu'ils ne concernent pas directement une entité comme la Ville de Genève. Il demande donc si la problématique du hacking se pose de la même manière en Ville et si le développement des logiciels libres a une incidence sur la sécurité informatique. M. Favre explique qu'il peut y avoir du piratage de données par inadvertance et donne l'exemple d'un cas en Angleterre où la cause était matérielle, en l'occurrence l'oubli d'un CD dans le métro! Il cite également le cas de l'Etat où une page sur le web avait été piratée mais ces situations, il convient de le préciser, sont relativement exceptionnelles et les entreprises ou les administrations publiques n'ont pas intérêt à vendre la mèche et restent le plus souvent discrètes là-dessus. M. Favre relève que les logiciels libres mettent à disposition des personnes intéressées leur code source et n'importe qui peut ainsi prendre connaissance des failles et pièges qui peuvent se produire dans un système. Il ajoute que ces logiciels sont systématiquement mis à jour et précise que 80% des serveurs de la DSIC sont équipés de logiciels libres. Ce même commissaire relève que les motionnaires avaient parlé du coût que cela représentait dans les entreprises et prend, à titre d'exemple, la société Kudelski qui investit des millions de francs pour la sécurité de son système informatique. Il se demande s'il y a vraiment une relation de cause à effet entre ces investissements et la protection effective des données. M. Favre explique qu'une entreprise telle que Kudelski ne peut effectivement pas se permettre de ne pas protéger de la manière la plus complète son système, ce qui n'est pas exactement le cas d'une administration publique comme la Ville de Genève qui ne dispose pas de données aussi sensibles.

Un commissaire ne saisit pas, en revanche, pourquoi la Ville n'a pas procédé à un audit systémique de son réseau? M. Maudet rappelle que la DSIC a mis en place 27 audits pendant ces deux dernières années dont 16 sectoriels, les autres étant plus globaux. Il n'y a donc pas là une approche uniquement spécifique, mais bien également des contrôles portant sur l'ensemble. La démarche va tendre à se globaliser avec la mise en place d'un nouveau site web interactif de la Ville de Genève au cours de l'année prochaine. Il est évident, à ce sujet, qu'une évaluation générale de la qualité du système sera entreprise avant l'ouverture de ce site. M. Favre rebondit sur cette question en précisant qu'en dehors des audits globaux

réguliers, on procède à des contrôles plus spécifiques à chaque nouvelle modification partielle du système. Il énonce que les audits systémiques sont onéreux, alors que les autres sont tout autant efficaces et extrêmement rapides à mettre en place. Ce même commissaire lui rétorque que précisément la motion propose de procéder à un audit global à la fois large et précis et s'étonne de la résistance qu'il perçoit du côté de la DSIC. M. Maudet ne comprend pas le procès d'intention qui lui est fait. Il tient à préciser que son département n'entend pas «jeter l'argent par les fenêtres», que de nombreuses démarches sont, d'ores et déjà, entreprises avec succès, mais que bien évidemment si le Conseil municipal souhaitait ajouter un demi-million au budget il n'allait pas se montrer moins royaliste que le roi et s'y opposer. Il n'est toutefois pas du tout certain que les résultats obtenus, ce faisant, soient significatifs ou supérieurs aux évaluations régulières qui sont actuellement entreprises régulièrement par la DSIC. M. Favre rappelle la proposition qu'il a faite d'associer quelques conseillères municipales et conseillers municipaux à la réalisation d'un audit afin d'en comprendre tous les tenants et aboutissants.

Un motionnaire estime qu'un auditeur peut aider la DSIC dans un certain nombre de démarches et notamment pour celles qu'elle a de la peine à remplir actuellement vis-à-vis des spams que les membres du Conseil municipal reçoivent régulièrement. Il pense également qu'un audit systémique permettrait de mieux définir les besoins en termes de ressources qui pourraient lui être affectées. Il se demande aussi, par rapport aux places de travail, si du personnel serait susceptible de vérifier l'utilisation conforme des mots de passe dans les services. Il estime donc, pour tous ces problèmes précis, qu'un audit général ne peut qu'intéresser la DSIC et lui recommande par conséquent d'entrer en matière. M. Favre lui répond que le problème posé par un audit de ce type est qu'il va mobiliser une grande partie du personnel qui ne va plus pouvoir assumer ses autres tâches courantes. C'est pourquoi la DSIC préfère procéder à des révisions successives et sectorielles afin de ne pas perturber le fonctionnement général du service. M. Sanchez demande si l'un de ces audits a fait apparaître de façon pertinente un certain manque de personnel à la DSIC. M. Maudet attire l'attention des conseillères municipales et conseillers municipaux sur le fait que précisément il demande le renforcement de l'effectif des collaborateurs et collaboratrices de la DSIC dans le projet de budget 2009 dans le but d'améliorer sa sécurité et son fonctionnement. M. Favre lit l'extrait d'un article dans lequel il ressort que les démarches entreprises par la DSIC sont largement pertinentes.

Une commissaire aimerait connaître le point de vue de la DSIC en ce qui concerne le considérant qui énonce que «plus de 50% des entreprises françaises ont été piratées, bien que ce pays soit plus avancé que la Suisse en matière de sécurité informatique». M. Maudet relève effectivement que ce considérant le rend sceptique. Il ne comprend pas très bien d'où il sort et s'étonne de ce type d'argument mal étayé. M. Favre estime qu'il faut prendre quelques cautèles avec

ce type d'énoncé. Il n'est pas précisé de quelles attaques il s'agit, mais ce qu'il en sait ne met pas la France en position de supériorité et, pour tout dire, il a le sentiment que c'est du pareil au même.

Une commissaire pense à la mise en place du vote électronique en stipulant que la Ville y sera très directement intéressée et s'interroge quant à la sécurité du choix des électeurs et électrices. M. Maudet rappelle que le peuple genevois va devoir se prononcer à ce sujet, mais attire toutefois l'attention de M^me^ Ecuyer sur le fait que ce n'est pas la Ville qui va procéder à ce contrôle, mais l'Etat lui-même.

Un commissaire aimerait connaître quel est l'équivalent des normes ISO pour la sécurité informatique en matière bancaire. M. Favre lui répond qu'il s'agit des normes ISO 27001.

Une commissaire demande à M. Favre si un audit «extraordinaire» n'apporterait pas quelque chose de plus pour la DSIC. M. Favre lui répond que la méthode de la DSIC qui consiste à diriger les audits par secteurs est efficace et rapide, alors qu'un audit général coûterait plus cher et prendrait plus de temps.

Un commissaire demande comment la DSIC procède pour les choix de mandataires, notamment en matière d'adjudication. M. Favre lui répond que les audits qui sont effectués tournent autour de 150 000 francs. Ces coûts permettent d'éviter un appel d'offres trop visible et donc de limiter le nombre d'informations demandées. La DSIC travaille avec un certain nombre de sociétés. Il y a eu entre 5 et 10 prestataires différents pour les 27 révisions parmi lesquels, à titre indicatif, les sociétés IBM et Hewlett Packard. La DSIC travaille en fonction du profil des entreprises, sachant que la plupart de ces sociétés offrent également leurs services à l'Etat et travaillent de concert avec le CTI. M. Maudet ajoute que le but est également de soutenir les entreprises genevoises en attribuant les marchés à différents mandataires.

Le président aborde le point relatif aux éventuelles auditions complémentaires souhaitées par la commission. Il suggère à la commission d'entendre un spécialiste privé de la sécurité informatique. Cette proposition est mise aux voix. A égalité des voix, le non l'emporte; cette audition est refusée par 6 non (1 AGT, 3 Ve, 1 R, 1 S) contre 6 oui (2 UDC, 2 L, 2 DC).

Un commissaire propose ensuite l'audition d'un fonctionnaire du Département des constructions et des technologies de l'information. Cette proposition est acceptée par 8 oui (2 DC, 1 S, 2 L, 1 R, 2 UDC) contre 3 non (Ve) et 1 abstention (AGT).

Le président propose également d'entendre un spécialiste de la brigade de la criminalité informatique. Cette proposition acceptée par 7 oui (2 DC, 2 L, 1 R, 2 UDC) contre 3 non (Ve) et 2 abstentions (1 S, 1 AGT).

Séance du 5 janvier 2009

Audition de M. Jean-Marie Leclerc, directeur général du Centre des technologies de l'information (CTI)

M. Leclerc a bien lu cette motion qu'il trouve tout à fait judicieuse car il estime que le problème de la sécurité est fondamental. Il n'a donc pas de commentaires particuliers à faire d'entrée à ce sujet et se montre prêt à répondre à toutes les questions.

Un motionnaire explique d'emblée que cette motion n'entend pas remettre en cause le fonctionnement général de la DSIC, mais corriger la pratique actuelle concernant la sécurité informatique. Il précise que devant la quantité d'attaques dont elle est la cible, il a jugé utile de proposer des audits externes en vue d'améliorer la situation présente. Il aimerait donc connaître la politique du CTI en la matière. M. Leclerc parle de ce que l'Etat fait dans ce domaine. Il énonce en premier que le CTI n'a pas recours à l'autorégulation systémique en ce qui concerne le contrôle car son service ne souhaite pas être juge et partie dans le domaine de la protection des données. Le CTI fait donc régulièrement appel à des sociétés externes qui auditent périodiquement les systèmes de son réseau.

Une commissaire demande à M. Leclerc ce qu'il pense de la première invite faisant référence à l'Etat qui figure dans la motion. Elle aimerait savoir si cela existe et si par conséquent le Canton reconnaît des entités indépendantes et privées. M. Leclerc relativise le contenu de cette affirmation en rappelant que l'Etat se comporte comme toutes les administrations publiques et qu'il doit notamment respecter l'Accord intercantonal sur les marchés publics (AIMP). Il poursuit en relevant que le CTI et la DSIC entretiennent de très bonnes relations et que, dans ce cadre, des échanges d'information ont régulièrement lieu en ce qui concerne les mérites ou défauts de telle ou telle société. Il précise toutefois que la qualité de ces entreprises varie continuellement en fonction d'un certain turnover qui prévaut dans ces sociétés.

Un commissaire aimerait savoir comment l'Etat apprécie la gestion des risques en termes quantitatifs et budgétaires. M. Leclerc précise que la sécurité absolue aurait un coût exorbitant et qu'il convient donc de travailler de façon ciblée. Le CTI a cartographié les différents systèmes utilisés et repéré ceux qui disposaient de données particulièrement sensibles. Il cite notamment celui qui est associé au dépouillement centralisé qui présente une importance particulière. Il remarque à ce sujet que l'appréciation des risques est évolutive. Une alerte à la bombe était auparavant hautement improbable alors qu'aujourd'hui elle ne saurait être éludée. On évalue par conséquent les risques en fonction d'une certaine cartographie qui se modifie continuellement. Il prend à cet égard l'exemple des spams qui connaissent un développement exponentiel. Le CTI en détruit chaque jour près de 65 000, ce qui correspond à un taux de décontamination de l'ordre de 98%. Le troisième élé-

ment consiste à mettre en place un processus de fabrication de réponse à la question en sécurisant une opération du début à son terme et M. Leclerc de prendre à titre d'exemple l'e-voting. Fort de ces paramètres, l'Etat décide des moyens financiers qu'il convient de mettre régulièrement à disposition du CTI.

Ce même commissaire souhaiterait également connaître la hauteur des sommes allouées pour ces audits internes en les comparant à ceux effectués par d'autres collectivités publiques de notre pays. M. Leclerc lui rétorque que la cartographie a été établie par le seul CTI qui, en termes de stratégie, doit définir ses propres options. Le recours à des entités externes doit être proportionnel à l'importance ou à la qualité des projets. Il n'est évidemment pas question, par exemple, d'avoir recours à des sociétés privées pour mettre en place l'e-voting. Il indique par ailleurs que le montant dévolu aux audits externes se situait en 2008 autour d'environ 150 000 francs.

Un motionnaire désire savoir s'il existe une certification pour les sociétés pratiquant des audits. M. Leclerc relève que l'Etat n'a pas la prétention d'attribuer des certificats à des sociétés privées mais qu'il dispose par contre d'un certain nombre de critères qui lui permettent d'opérer des choix.

Un commissaire relève que la Ville de Genève agit un peu de la même manière en procédant à de petits audits pour chaque module mis en ligne mais aimerait savoir si l'Etat s'intéresserait à un audit portant sur l'ensemble de son système informatique. M. Leclerc remarque que les accidents procèdent plus de l'erreur humaine que de véritables défaillances techniques. Il convient donc à cet égard d'avoir, d'une part, des approches spécifiques mais, d'autre part, d'entreprendre des évaluations plus globales qui portent sur le fonctionnement même de l'administration. En ce sens-là, il partage le point de vue du président.

Un commissaire aimerait savoir si l'Etat recourt systématiquement aux mêmes prestataires et connaître la logique qui prévaut dans ce domaine. M. Leclerc rappelle que l'Etat respecte les règles AIMP d'attribution des marchés et qu'il procède donc à des appels d'offre mais ajoute qu'il évite pour des raisons de sécurité interne d'avoir recours plusieurs fois de suite aux mêmes sociétés. Ce roulement des entreprises permet au CTI de conserver une certaine indépendance. Ce même commissaire se demande s'il ne serait pas plus pertinent de confier certaines missions à un seul et même prestataire afin de mieux cerner dans la durée les problèmes de sécurité informatique. M. Leclerc énonce que le CTI ne confie pas un même mandat à plusieurs sociétés en même temps. Ces audits, comme il l'a indiqué précédemment, portent sur des missions spécifiques, mais même s'il s'agissait d'entreprendre un contrôle plus global, la procédure d'attribution, comme il l'a déjà relevé, resterait la même. D'ailleurs cela arrive et récemment il a mandaté une société afin de contrôler l'organisation interne de tout un service. Il n'est par contre pas très signifiant de confier un mandat global à une société

sur la sécurité car ce problème est récurrent et donc cette mission, tel le mythe de Sisyphe, serait perpétuellement à reprendre. Il ne peut donc s'agir là que de mandats spécifiques portant chaque fois sur un champ précis. Il ajoute qu'il n'est pas toujours nécessaire de mandater un prestataire pour procéder à un audit lorsque par exemple il s'agit de contrôler des utilisateurs qui utilisent à des fins personnelles l'équipement informatique mis à leur disposition.

Une commissaire, prenant le contre-pied des motionnaires, rappelle que la DSIC, sous l'autorité de son excellent directeur M. Eric Favre, a procédé à 27 audits internes ces deux dernières années et se pose la question de la pertinence d'une intervention politique, que ce soit à la Ville ou à l'Etat dans le domaine de la sécurité informatique. M. Leclerc partage entièrement l'avis de la préopinante en ce qui concerne les qualités de M. Favre avec qui il entreprend d'ailleurs une collaboration tout à fait fructueuse. Il ajoute toutefois qu'en tant que responsable du CTI, il est de son devoir de proposer des crédits en vue de sécuriser le système informatique de l'Etat. Il ajoute qu'il est souhaitable de conserver une certaine humilité face au problème de la sécurité et pense utile de le faire partager aux autorités exécutives et législatives. Il prend à titre d'exemple une récente audition par la commission de l'enseignement où on lui a demandé s'il était possible de prendre techniquement des dispositions pour empêcher des élèves d'accéder à des sites pornographiques. Il n'a pu que répondre que le sujet ne passait pas uniquement par la seule augmentation d'un crédit en vue de garantir cette sécurité, mais également par l'implication des enseignants et la responsabilisation des acteurs concernés.

Une commissaire, prenant appui sur le taux de 98% de décontamination des spams, demande dans quelle mesure il est possible de prévenir les failles qui apparaissent au fur et à mesure. M. Leclerc relève qu'à la minute où il parle, aucun virus dangereux n'a infecté le réseau de l'Etat, mais bien évidemment il n'est pas certain de pouvoir dire la même chose demain ou plus tard. Toutefois, il peut affirmer que de sérieuses perturbations ne pourraient se produire car toutes les mesures de prévention utiles et nécessaires ont d'ores et déjà été prises.

Un commissaire revient sur l'invite qui concerne le choix des mandataires. Il souhaiterait connaître leur nombre, savoir si la Ville a systématiquement recours aux mêmes entreprises, si le CTI suit la situation interne de ces sociétés et si, compte tenu de l'ouverture des marchés publics, des entreprises étrangères peuvent être mandatées par l'Etat. M. Leclerc répond négativement à la dernière question pour la raison suivante: Genève dispose d'un pôle de compétences privées ou publiques exceptionnel sur son territoire et il convient donc, dans le domaine de la sécurité informatique, de partager les mêmes connaissances en matière de fonctionnement juridique et politique. Il indique, à cet égard, que des mandats ont été confiés à l'Université et à l'Ecole polytechnique et que ces institutions n'ont pas ménagé leur temps en vue d'obtenir d'excellents résultats.

Un commissaire constate que la Ville va mettre en ligne un guichet unique comme à l'Etat et aimerait en somme savoir si M. Leclerc estime qu'elle est suffisamment armée pour affronter ce cap technologique? M. Leclerc rappelle que le CTI et la DSIC s'échangent un grand nombre d'informations et qu'ils travaillent en complète synergie. Il est donc par conséquent persuadé que toutes les mesures utiles et nécessaires seront prises pour la mise en place de ce guichet unique. Il ajoute qu'à cet égard un cadre a été défini par la Confédération comportant un certain nombre de règles impératives auxquelles sont soumises toutes les collectivités publiques. Il ajoute que la Confédération, le Canton et la Ville ont déjà élaboré ensemble une approche pour que les délégations de compétences se fassent avec les mêmes types de technologie dans le but d'éviter des failles simultanées dans plusieurs systèmes. Fort de cet état de choses, M. Leclerc estime que la démarche entreprise par la Ville lui paraît tout à fait conforme aux normes de sécurité établies par les autorités fédérales et cantonales.

Une commissaire, constatant que la motion présentait un caractère alarmiste, demande à M. Leclerc si les tentatives de piratage sont nombreuses à l'Etat et si les «hackers» sont plus incisifs qu'auparavant. M. Leclerc indique que l'on est passé d'un aspect ludique – et il fait référence à un étudiant qui à partir d'un «Joyeux Noël» avait pu pénétrer dans les serveurs de la NASA – à des démarches volontaristes qui visent à infiltrer des réseaux en vue de détourner des montants de monnaie scripturale. Il considère toutefois que le danger à l'Etat porte moins sur des détournements financiers que sur des tentatives visant à porter un préjudice politique par le biais de l'accaparement de certains serveurs. C'est un élément bien réel qu'il faut néanmoins relativiser car les ingénieurs qui travaillent au CTI ont proportionnellement également augmenté leur niveau de compétence. C'est la raison pour laquelle il convient d'engager de nouveaux collaborateurs et de nouvelles collaboratrices très aguerris-e-s sortant des écoles d'ingénieurs afin d'ajuster les connaissances des personnes qui travaillent au CTI.

Une commissaire estime que la sécurité de l'e-voting devrait être en soi parfaite. Elle se demande si l'e-voting sera plus sûr que le vote par correspondance. M. Leclerc manifeste une grande confiance dans l'e-voting pour la raison que le CTI a procédé à onze expériences successives en congruence avec des démarches entreprises simultanément dans plusieurs pays d'Europe. La dernière expérience a associé un-e représentant-e par parti politique en créant une 46^{e} commune électorale virtuelle et les participants-e-s ont pu ainsi constater la parfaite symétrie qui prévalait entre leur vote traditionnel et l'e-voting. Le CTI a, par ailleurs, travaillé avec l'Université de Genève qui a pu pousser très loin des expériences en physique quantique montrant à l'évidence que le système envisagé était très performant. Certes, il serait présomptueux d'affirmer que les risques n'existent pas du tout mais, en l'état des choses, l'e-voting se présente comme un processus qui offre de grandes garanties de protection des données aux électeurs et électrices.

M. Leclerc se montre, par voie de conséquence, serein et considère qu'il convient d'être entièrement rassuré sur ce plan-là.

Un commissaire, faisant référence à l'un des considérants qui parle de piratage d'une banque, aimerait connaître quelques exemples d'infiltration vis-à-vis d'une collectivité publique puisque ceux-ci semblent plus rares. M. Leclerc, hormis quelques indiscrétions volontaires en direction de la presse, n'a pas d'exemples sérieux à citer de tentatives de blocage du réseau par des «hackers».

Une commissaire demande si des informaticiens du CTI participent aux concours de «hacking» qui ont lieu chaque année. M. Leclerc lui répond que les ingénieurs du CTI ont l'obligation de se mettre à la page, mais qu'ils ne participent pas à ces concours pour des raisons à la fois éthiques et budgétaires. M. Leclerc indique que des formations certifiantes sont régulièrement proposées à ses collaborateurs et collaboratrices et concernant plus largement l'ensemble des utilisateurs et utilisatrices, deux cours sont proposés, l'un portant sur la connaissance et l'utilisation des PC et l'autre traitant de la sécurité informatique. Pour réaliser cet objectif, le CTI a attribué à chaque département un collaborateur ou une collaboratrice qui participe à la mise en place de mesures de sécurité et qui assure ainsi une liaison permanente avec la direction du CTI.

Le président remercie M. Leclerc de sa participation et de la qualité des réponses qu'il a pu fournir à la commission.

Séance du 19 janvier 2009

Audition de M. Alain Bondet, officier de sécurité des systèmes informatiques au Service de coordination informatique de la police

M. Bondet n'a pas de remarques préliminaires à présenter et se déclare prêt à répondre aux questions.

Un commissaire lui demande si les considérants de la motion lui paraissent pertinents. M. Bondet relève que les chiffres présentés sont exacts, voire sous-évalués car nombre d'entreprises piratées se gardent bien de dire qu'elles l'ont été.

Un commissaire a eu l'occasion de discuter avec une personne spécialisée dans les audits de systèmes informatiques qui lui a dit qu'il était en réalité assez facile d'accéder à peu près partout dans des délais extrêmement courts. Il aimerait savoir si M. Bondet partage ce point de vue. M. Bondet confirme en remarquant qu'il existe sur le marché des kits prêts à l'emploi. Il y a dans ce domaine des sites qui permettent leur hébergement et qui sont installés dans des pays peu respectueux des lois internationales. Il existe à cet égard des pirates disposant d'une

licence en bonne et due forme qui leur permet de vendre leur logiciel bien abrités derrière ce paravent.

Une commissaire aimerait savoir comment il est possible de vendre des outils informatiques qui s'apparentent à des armes et comment des banques peuvent se livrer à ce commerce en se prêtant à ces transactions. M. Bondet constate que ces ventes sont en principe interdites mais que dans les faits elles peuvent avoir lieu car elles ignorent les frontières existant entre les différents pays.

Une commissaire demande à M. Bondet comment il fait pour disposer d'un système performant à la police. M. Bondet indique qu'il s'en tient à la norme ISO 27002 qui propose un certain nombre de points à respecter pour balayer le périmètre complet de la sécurité informatique. Il convient de ne pas encombrer le réseau d'une sécurité excessive, mais de se situer dans un juste milieu qui évite d'éventuels blocages des systèmes. Dans cet esprit, il faut donc accepter des risques potentiels car la sécurité absolue n'existe pas, et se mettre constamment à jour face à l'évolution rapide des méthodes de piratage.

Cette même commissaire rebondit en constatant que les «hackers» sont de plus en plus performants en cherchant toutes les failles possibles et demande comment la police réagit face à cette explosion du piratage. M. Bondet confirme en indiquant que des failles peuvent se présenter dans les logiciels, dans les réseaux, voire chez les utilisateurs eux-mêmes. Il relève d'ailleurs que le facteur humain est à la base d'un bon 80% des erreurs qui permettent aux pirates de pénétrer dans les réseaux.

M^me^ Arlotti poursuit en citant un piratage de passeport biométrique qui avait permis à des «hackers» de placer des données dans la puce liée au document et se demande même s'il convient de mettre en place des systèmes informatiques sécurisés qui se révèlent en fin de compte peu fiables, en considérant en particulier à l'e-voting. M. Bondet remarque qu'il convient d'évaluer le niveau de risque acceptable tout en restant dans les moyens financiers mis à disposition. Il est par conséquent nécessaire de proposer un audit avant la mise en place de chaque nouvelle application. Il est, dans cette idée, opportun d'évaluer chaque fois le degré de protection à installer dans un nouveau système et l'e-voting fait évidemment partie des objectifs prioritaires. Il ajoute que les failles ne sont pas toujours le fait de pirates, mais qu'elles peuvent tout simplement être techniques et demander une simple réparation mécanique.

Un commissaire aimerait connaître l'appréciation de M. Bondet en ce qui concerne la motion, en particulier au sujet des mandats confiés à des sociétés externes. M. Bondet explique à la commission que pratiquement tous les mandats attribués par la police sont confiés à des entreprises privées et le problème réside essentiellement dans la confiance que l'on peut faire à ces mandataires. Il estime

que la part dévolue à la sécurité représente un ratio compris entre 10 et 20% de l'ensemble des moyens mis à sa disposition. Ce même commissaire renchérit en souhaitant avoir des informations plus concrètes sur ces moyens financiers en regard avec ceux qui sont octroyés dans d'autres cantons et sur la fréquence de ces audits. M. Bondet n'a pas de chiffres à donner compte tenu de l'organisation qui prévaut dans les différents cantons. Il relève sur ce plan que, par exemple, le canton de Vaud comporte une police cantonale, mais également municipale en Ville de Lausanne. Il y a d'autre part des cantons qui gèrent leur informatique de façon centralisée et d'autres qui répartissent ces charges dans les différentes administrations, police comprise. Il ajoute que les systèmes d'information sont parfois dissemblables et constate en conséquence qu'il est impossible de procéder à des comparaisons significatives. Il termine en indiquant que le dernier audit global des systèmes d'information de la police genevoise a eu lieu en 2007 et souhaiterait que ces contrôles ne soient pas effectués de manière ponctuelle, mais cyclique. Les différents points de la procédure à suivre en sont les suivants:

– la politique de sécurité de l'entreprise;
– l'organisation de la sécurité;
– la classification en propriété des actifs;
– la sécurité du personnel;
– la sécurité physique et environnementale;
– l'exploitation des systèmes et des réseaux;
– le contrôle des accès logiques;
– le développement et la maintenance;
– la continuité des services;
– la conformité avec le code légal et technique.

Ce commissaire demande encore si la mise en place du cycle a déjà commencé. M. Bondet précise que ce n'est pas encore le cas et que son service est en train de travailler sur les résultats de l'audit précédent en collaboration avec le CTI.

Un commissaire revient sur les distinctions faites par M. Bondet en ce qui concerne l'aspect technique et le facteur humain et se demande si ce dernier terme comprend le comportement des personnes. M. Bondet acquiesce en ajoutant que cela commence, dès l'engagement, par un complément de formation et l'acceptation d'une charte d'utilisation.

Une commissaire ne voit pas l'intérêt pour des «hackers», en dehors du secteur des contraventions, de pénétrer dans les réseaux de la police et souhaiterait avoir le point de vue de M. Bondet à ce sujet. M. Bondet explique qu'il y a un certain nombre de cas dans lesquels des «hackers» pourraient tirer profit d'un

piratage informatique et de citer, à titre d'exemple, l'organisation des mesures préventives concernant la manifestation contre le WEF. Il ajoute, d'autre part, que la connaissance de certaines données sensibles de police peut avoir des conséquences dramatiques sur la sécurité des biens et des personnes.

Un commissaire souhaiterait connaître le point de vue de M. Bondet en ce qui concerne les données les plus sensibles intéressant les pirates, voire un classement des priorités vues sous l'angle de la police. M. Bondet retient en particulier la sécurité bancaire, les données fiscales des personnes physiques ou morales, et nombre d'autres informations confidentielles. Il relève que l'infiltration des réseaux est relativement simple et prend l'exemple de prétendus étudiants qui, posant des questions par le biais d'un fichier Excel qui, lorsqu'il est renvoyé, leur permet de pénétrer ainsi dans le réseau. On voit là que l'accent est à mettre sur la formation du personnel afin d'éviter de répondre à ce genre de sollicitation.

Un commissaire demande si M. Bondet connaît des cas de collectivités publiques qui ont été piratées. M. Bondet lui donne l'exemple des sites admin.ch et Swisscom qui avaient été infiltrés et rappelle que des administrations américaines ont fait l'objet d'attaques en règle. Ce commissaire poursuit en souhaitant savoir si des tentatives de piratage d'administrations publiques ou internationales ont abouti et on été portées à la connaissance de public. M. Bondet indique qu'il y a quelques années les données personnelles des cartes de crédit des participants-e-s au WEF avaient été piratées.

Un commissaire aimerait savoir si M. Bondet est habilité dans le cadre des normes AIMP à choisir les entreprises compétentes afin d'auditer son service. M. Bondet lui répond par l'affirmative tout en précisant que c'est son prédécesseur qui a attribué les adjudications précédentes. Il va donc reprendre ce dossier avec le responsable sécurité et système d'information (RSSI).

Un commissaire demande comment s'opère le choix de la société mandatée. M. Bondet lui répond que ces choix se font en concertation avec les autres responsables de sécurité informatique à l'Etat et donne, à titre indicatif. les noms de NetExpert et de HackNet SA.

Le président demande à la commission si d'autres auditions sont souhaitées.

Un commissaire, à la lumière des récentes auditions, souhaite réentendre le magistrat afin de pouvoir revenir sur certains points, notamment sur la cartographie des risques et les comparaisons avec d'autres collectivités publiques. Un commissaire estime que la commission pourrait demander des compléments d'information en ce qui concerne la formation dispensée au personnel de la Ville. Une autre commissaire relève que les conseillères municipales et les conseillers municipaux n'ont pas reçu de formation appropriée en ce qui concerne ces problèmes de sécurité.

Votes

Le président revient sur les auditions et met aux voix celle d'une entreprise spécialisée dans la sécurité informatique. Cette audition est acceptée par 7 oui (1 DC, 1 AGT, 2 L, 2 UDC, 1 R) contre 3 non (Ve) et 3 abstentions (2 S, 1 AGT).

Le président va donc prendre des contacts dans ce sens. Il propose ensuite l'audition du magistrat et de son service. Cette audition est acceptée par 8 oui (2 S, 2 AGT, 1 DC, 2 L, 1 UDC) contre 1 non (R) et 4 abstentions (3 Ve, 1 UDC).

Le président propose alors l'audition des services hors magistrat, qui est refusée par 4 non (2 S, 1 AGT, 1 R) contre 2 oui (1 DC, 1 UDC) et 7 abstentions (3 Ve, 1 AGT, 2 L, 1 UDC).

Le président met aux voix l'ordre de priorité. Un commissaire pense préférable, afin de disposer de tous les éléments, d'entendre en premier la société. La proposition de M. Rubeli est acceptée à l'unanimité.

Une commissaire informe la commission que le concours de «hacking» aura lieu le 6 février à 18 h à l'Ecole d'ingénieurs.

Séance du 2 mars 2009

Audition de M. Lorin Voutat, administrateur, et de M. Pierre Polette, directeur de la Société Ilion Security SA

Le président demande à M. Voutat et M. Polette de se présenter. M. Voutat est le cofondateur et administrateur de la société Ilion Security SA. M. Polette en est le directeur général et le président du conseil d'administration. M. Voutat entreprend de présenter la société Ilion Security SA. Cette entreprise a été créée en 2002 à partir du besoin avéré pour certaines multinationales d'évaluer les attaques informatiques dont elles étaient la cible et de mettre en place des recommandations afin de s'en prémunir. La société Ilion Security SA ne vend pas de produits informatiques, mais réalise des audits et donc propose des conseils en sécurité et en intégration à ses clients. A titre d'exemple, sa société a été mandatée par l'Etat de Genève pour évaluer le niveau de risques du système e-voting; elle travaille également de façon périodique pour la Confédération et en particulier pour Arma Swiss.

M. Polette indique pour sa part qu'il dirige cette société depuis quinze ans et qu'il travaille comme consultant et expert en France auprès de plusieurs banques et de nombreuses collectivités locales et notamment de plusieurs grandes villes ainsi que des départements. M. Voutat ajoute que son entreprise a été mandatée afin d'auditer les systèmes informatiques des HUG, en collaboration avec les services de M. Leclerc et le Département des constructions et des technologies

de l'information. Il relève à cet égard que sa société ne tient pas à concurrencer l'excellent niveau en informatique des personnes qui travaillent à l'Etat, mais au contraire à les accompagner et à mettre en évidence la qualité de leur travail.

Le président ouvre le tour des questions et prend d'entrée la parole en lui demandant si Ilion Security SA a déjà travaillé pour la Ville de Genève. M. Voutat lui répond par la négative.

Une commissaire voudrait des précisions en ce qui concerne les produits de sécurité et d'intégration. M. Polette indique que son entreprise s'occupe de prestations de service dans le sens de conseil et d'audit. Il ne vend pas de produits informatiques (logiciels, antivirus, firewall etc) puisqu'ils existent d'ores et déjà sur le marché. Le mot «intégration» signifie la mise en place adéquate de ces produits. Dans ce sens, la société Ilion Security SA peut procéder à des appels d'offre afin de trouver les logiciels de sécurité adéquats pour les clients qui souhaitent s'en procurer. Cette même commissaire demande si sa société est à même d'étudier des solutions aux problèmes techniques révélés suite aux audits. M. Polette lui énonce que ce n'est pas le cas. Son travail consiste à mettre le doigt sur les problèmes et non à réparer les systèmes infiltrés. M. Voutat précise que leur but premier est de faire une analyse rapide du réseau et dans un deuxième temps de proposer les produits proposés par les différents grands groupes de sécurité informatique. Il relève en revanche que les autres sociétés qui prétendent pouvoir réaliser des audits ont généralement pour but de vendre des logiciels en sécurité informatique. Ceci explique que la plus grande difficulté d'Ilion Security SA réside dans le recrutement de ses ingénieurs, compte tenu du haut degré d'évaluation demandé dans le domaine de la gestion des risques informatiques. Tous les collaborateurs et toutes les collaboratrices de sa société sortent de l'EPFL ou des hautes écoles européennes, mais il ajoute que, et loin s'en faut, tous et toutes n'ont généralement pas au départ tout le bagage requis pour cette fonction et que beaucoup de choses s'apprennent, comme l'on dit généralement, sur le tas, au cours d'une année de formation en emploi. Pour donner un exemple de la qualité des services offerts par sa société, il cite l'audit qu'elle a réalisé pour Arma Swiss, alors même qu'elle se trouvait en concurrence avec trois autres entreprises suisses allemandes, lorsqu'on sait qu'au-delà de la Sarine on fait souvent peu de cas des Suisses romands...

Un commissaire évoque que la Ville de Genève procède à une trentaine d'audits externes par année et se pose donc la question de l'efficience de ces contrôles. M. Voutat ne connaît pas les attentes de la Ville de Genève en la matière, mais pense que cette différence peut s'expliquer par le fait que la Ville est moins exposée au «hacking» que l'Etat ou les banques. Il ajoute que la Ville a probablement aussi des demandes très spécifiques sur ses systèmes et comprend par conséquent qu'elle ait recours à des sociétés moins importantes en précisant que les audits haut de gamme peuvent coûter assez cher.

Un commissaire, prenant l'exemple de l'e-voting, dans lequel la gestion des risques doit être maximale, voudrait savoir de quelle manière la cartographie a été établie, compte tenu de la multiplicité et de l'importance des risques encourus en regard avec la Ville de Genève qui ne dispose pas, quant à elle, de données aussi sensibles que l'Etat dans le domaine fiscal ou la protection des données. M. Polette explique que l'on procède à une classification des données, car certaines sont moins importantes que d'autres. Il indique, à titre d'exemple, que des collectivités qu'il a pu auditer n'ont pas souhaité que certaines de leurs activités soient mises sur la place publique, notamment dans le domaine des investissements, et renverse la question en demandant à la commission si des données politiques concernant les commissaires et relatives à leurs propos ou leurs attitudes doivent être nécessairement connues du grand public. Il donne, à cet égard, l'exemple de vols d'identifiants de personnes qui peuvent se faire passer pour d'autres. M. Voutat précise que sa société pourrait mettre en évidence les risques, mais insiste sur le fait qu'en dernier ressort c'est aux autorités politiques de prendre de bonnes décisions.

Un commissaire aimerait avoir quelques exemples d'audits effectués auprès de collectivités publiques par Ilion Security SA. M. Polette indique qu'Ilion Security SA est auditeur permanent de la Ville de Lyon, du département du Rhône ainsi que de la communauté urbaine du grand Lyon. Il y travaille notamment sur la charte d'utilisation d'Internet dans le but de limiter son utilisation au sein des administrations publiques. Renvoyant la question, il demande à la commission si, lors des votations à Genève, l'informatique est mise à contribution. Un commissaire lui répond par l'affirmative. M. Polette souligne que le niveau de disponibilité est à cet égard très important car on comprendra bien que des données éludées peuvent avoir des conséquences sur les résultats électoraux.

Un commissaire aimerait connaître quelques exemples d'attaques subies par des collectivités publiques. M. Voutat prend l'exemple d'un conseiller d'Etat jurassien à qui on avait emprunté son e-mail pour expédier un message à l'intention d'un certain nombre de personnes dans lequel il était dit qu'il ne souhaitait plus reprendre le département dont il avait la charge. Ce piratage a eu pour effet d'annuler l'élection et d'obliger à en organiser une nouvelle.

Ce même commissaire remarque que le piratage informatique semble avoir des conséquences plus dommageables sur le secteur privé que sur le secteur public. M. Polette confirme que, bien évidemment, ce qui intéresse en priorité les pirates, ce sont les comptes bancaires et tous les codes qui sont liés aux cartes de crédit et aux ventes en ligne.

Une commissaire aimerait savoir si des clients d'Ilion Security SA reviennent en demandant si les mesures préconisées par la société prestataire ont été bien mises en œuvre. M. Polette confirme en indiquant qu'il est courant que des entités auditées rappellent son entreprise afin de mesurer l'efficience des mesures pré-

conisées. Des validations sont, à cet égard, effectuées généralement dans les cinq jours qui suivent la mise en place des correctifs proposés.

Une commissaire remarque que les sociétés auditrices emploient d'anciens hackers et se pose la question de la confiance qu'on peut leur accorder. M. Voutat considère que les ingénieurs haut de gamme, issus des grandes écoles, utilisés par certaines sociétés ont une grande palette de compétences parmi lesquelles, certes le hacking, mais également des connaissances qui vont bien au-delà. M. Polette ajoute que tout dépend de la maturité du personnel en question. Revenant sur la question de la multiplicité des prestataires, il estime qu'une meilleure gestion des risques passe par des mandats qui ne seraient confiés qu'à une ou deux sociétés plutôt qu'à un grand nombre.

Une commissaire demande si, de temps à autre, les budgets prévus sont dépassés pour l'étude d'un segment de système pouvant faire apparaître d'autres failles du réseau. M. Polette reconnaît que c'est souvent le cas, mais que son rôle est d'expliquer que dans le cadre d'un forfait l'on ne peut aller plus loin. M. Voutat qui revient sur les dépassements de budget considère que ce type de problème peut paradoxalement avoir des conséquences positives puisque ces dépassements sont liés à des insuffisances fonctionnelles qui peuvent trouver des solutions dans le cadre de l'expertise opérée par la société auditrice. Ces conseils peuvent donc produire un excellent retour sur investissement.

Séance du 9 mars 2009

Audition de MM. Pierre Maudet, conseiller administratif chargé du Département de l'environnement urbain et de la sécurité, et Eric Favre, directeur de la DSIC

Le président demande à M. Maudet s'il entend faire une déclaration liminaire. M. Maudet a bien compris qu'il s'agissait de donner avant le vote la position du Conseil administratif après tout le travail d'investigation effectué par la commission. M. Favre remet à titre informatif aux commissaires un certain nombre de rapports dont certains ont un caractère strictement confidentiel. Le premier document contient des réponses aux questions posées par la commission. Le second fascicule comprend des données assez sensibles sur des comparaisons entre différents cantons et ne peut donc rester dans les mains des conseillères municipales et conseillers municipaux. Il ne doit donc pas, pour ces raisons, figurer tel quel dans le rapport de la commission. Il y a enfin l'audit réalisé par la société Objectif Sécurité SA pour la DSIC ainsi qu'une présentation succincte de l'entreprise mandatée.

M. Maudet propose que la commission prenne un moment pour prendre connaissance des dossiers. Le président demande donc aux membres de la commission de les lire pendant une quinzaine de minutes.

Une commissaire a compris que la sécurité était ventilée à tous les niveaux de la DSIC et qu'elle concernait tous les collaborateurs et toutes les collaboratrices de ce service. Elle aimerait par conséquent savoir de qui l'on parle quand l'on dit que l'administration a un «pilote à son bord». M. Maudet comprend bien sa question et lui rétorque qu'elle a raison d'estimer que les problèmes de sécurité reposent sur chacun des collaborateurs de la DSIC. Il relève toutefois que cette motion et son titre ont semé le trouble dans ce service. Ce titre a été perçu comme une forme de défiance vis-à-vis du travail effectué par le personnel. Pour parler clair, «le pilote» dont on parle ici est M. Favre qui maîtrise bien l'ensemble des dossiers et en particulier celui de la sécurité informatique.

Une commissaire a une observation concernant la page 8 où il est dit tout au début «par comparaison, en Ville de Genève, le budget annuel moyen consacré à la sécurité informatique peut être estimé à environ 1,5 million de francs (y compris les locaux et le personnel), soit à 5,4% du budget global consacré aux systèmes d'information et de communication.» Elle remarque que ce ratio mis en regard du budget global de la Ville de Genève ne représente, dans les faits, que le 1‰ des montants affectés au fonctionnement. Elle a par contre une question concernant la directive relative à l'utilisation des systèmes d'information et de communication et demande si la Ville a réellement les moyens de l'appliquer aujourd'hui. M. Favre estime que cette directive, segmentée en différentes parties, qu'il a rédigée avec M. Olivier Burri est destinée surtout aux collaborateurs et collaboratrices de la DSIC. Elle pose le principe de ce que l'on attend de ce personnel qui jouit, par ailleurs, d'une certaine liberté d'action. Il juge au surplus que la DSIC dispose déjà d'un certain nombre de moyens pour contrôler la sécurité tout en respectant la sphère privée des personnes utilisant son réseau. M. Maudet, pour compléter cette information, indique qu'il y a eu quelques cas qui ont débouché sur des licenciements en regard de l'article 11 qui limite le droit d'accès à Internet.

Une commissaire fait référence aux différentes auditions qui ont eu lieu et remarque que le plus grand nombre de failles provient des utilisateurs eux-mêmes. Elle reprend l'exemple cité par Ilion Security SA qui indiquait qu'en laissant traîner une clé USB dans un local, on pouvait induire une pénétration massive d'un système. Elle demande donc si la DSIC dispose d'une marge financière suffisante pour procéder à des audits de qualité et aimerait connaître le nombre qui serait nécessaire pour que tout se passe bien. M. Maudet répète, pour mémoire, qu'il y a environ 58 000 attaques par année et qu'il convient de rester perpétuellement sur ses gardes. Il rappelle que la DSIC cherche en ce moment un ingénieur responsable de la sécurité qui placerait au cœur de sa réflexion les failles humaines potentielles en déchargeant ainsi le directeur qui assume actuellement cette responsabilité. C'est donc de cela que le magistrat a besoin en ce moment pour «dormir sur ses deux oreilles» et non d'audits externes supplémentaires. Le point sensible réside donc dans la qualité et l'éthique du personnel et c'est pour-

quoi M. Favre met l'accent sur sa formation. Pour en revenir aux audits, il n'a pas de problèmes financiers à cet égard, mais rappelle qu'il entend essentiellement mettre l'accent sur les ressources humaines à l'interne qui permettent de structurer la mise en place de la sécurité au sein de la DSIC. M. Maudet rappelle qu'il n'est politiquement pas hostile à des externalisations, mais relève que dans le cas présent le problème n'est pas là mais porte sur une réorganisation interne de la DSIC. Il indique que le dépôt de cette motion et de son titre en particulier ont conduit quatre sociétés à lui faire des offres d'audits externalisés. Il évoque donc la possibilité que cette motion soit elle-même un «cheval de Troie» qui aurait pour conséquence d'ouvrir quelques marchés à des sociétés en quête de mandats!

Une commissaire relève que dans ses documents confidentiels la DSIC évoque la mise en place de dispositifs en vue de limiter les risques en cas de catastrophe. Elle aimerait savoir desquels il pourrait s'agir. M. Favre explique que l'idée est de disposer de plusieurs serveurs situés dans différents secteurs de la ville de Genève géographiquement distants. Ceci pour permettre, par exemple dans le cas d'un tremblement de terre, de sauvegarder l'ensemble des données car si l'un d'entre eux devait être détruit, l'autre pourrait ainsi continuer à fonctionner. Il indique à cet égard que, dans cet esprit, un crédit sera prochainement proposé au Conseil municipal en vue de rénover le centre de calcul de la rue du Stand 25.

M. Maudet répète qu'il fait l'objet d'un certain nombre de pressions de la part d'entreprises privées dans le but d'auditer la DSIC, mais n'entend pas se laisser dicter ses choix stratégiques.

Une commissaire demande ensuite qui édite la norme ISO 27001. M. Favre lui répond qu'il s'agit de l'Organisation internationale de normalisation, qui établit les standards internationaux dont le plus connu est l'ISO 9000 relative à la gestion de la qualité. La série des ISO 27000 sont en rapport à la sécurité de l'information.

Un commissaire demande si la DSIC a enregistré une hausse des attaques depuis le dépôt de la motion. M. Favre l'informe que pour cette question il se base d'abord sur les flux qui donnent un aperçu général de la situation. Sur cette base il n'a rien constaté de particulier.

M. Maudet explique que le rapport confidentiel répond clairement à la motion et que son titre, «Cartographie des risques des systèmes d'information», est parfaitement explicite à cet égard. Il y a donc clairement une relation de cause à effet entre la motion et ledit rapport. Un commissaire conclut que si le Conseil administratif a procédé à un audit après que cette motion a été déposée c'est donc dire qu'elle avait tout son sens puisqu'elle a permis la production du présent rapport. M. Favre confirme que l'avantage de cette démarche est qu'elle a permis de produire un document facile à lire car il est vrai que la DSIC a tendance à présenter des rapports un peu trop techniques. Il considère que cette motion, en faisant

allusion à une entité indépendante et privée reconnue par l'Etat, autrement dit la société Ilion Security SA, n'est peut-être pas aussi innocente qu'elle n'en a l'air. Ceci dit, elle aura eu le mérite de sensibiliser la DSIC à la problématique des audits externes et de permettre aux membres de la commission de poser des questions pertinentes afin de se faire un point de vue sur le sujet. Il espère par conséquent, au travers du document confidentiel qui leur a été remis, avoir répondu à toutes questions légitimes qui ont pu être posées en matière de sécurité informatique. M. Favre estime tout à fait pertinent que la commission se soit penchée sur le problème de la sécurité, mais relève que le titre provocateur de la motion qui a fait réagir le personnel n'était peut-être pas forcément judicieux.

Une motionnaire tient à faire remarquer qu'elle regrette que l'intitulé de la motion ait pu froisser les collaborateurs et collaboratrices de la DSIC et précise que ce n'était évidemment pas là l'intention des motionnaires. Elle rappelle que l'idée était, en fait, d'appuyer le travail de la DSIC en confiant à des mandataires externes certaines tâches d'audit relatives à la sécurité à la fois interne et externe.

Discussions

Une commissaire AGT reconnaît que cette motion a permis à la commission de mieux comprendre le fonctionnement de la DSIC en matière de gestion des risques et, dans ce sens-là, elle a été utile. Par contre il est manifestement inutile de demander à la Ville de Genève de faire ou de refaire ce qu'elle fait déjà. C'est la raison pour laquelle son groupe refusera ladite motion.

Un commissaire socialiste indique pour sa part qu'il avait l'intention première de refuser cette motion, mais qu'au travers des documents reçus il apparaît que tout ne figure pas dans la cartographie proposée et qu'il trouverait dommage, à partir de tout le travail qui a été effectué dans la commission, que cette motion doive au final être refusée. C'est pourquoi, alors que sa collègue s'appuie sur une position politique qui repose sur un arbitrage entre la sécurité et la liberté, il s'abstiendra.

Une commissaire du Parti démocrate-chrétien considère que les nombreuses auditions ont permis de répondre à la motion. Il lui semble donc difficile de dire non alors même que la DSIC a clairement indiqué la marche qu'elle entendait suivre dans ce domaine. Prise donc entre la motion et la réalité, elle souhaiterait modifier le texte de l'invite de la motion qui proposerait au Conseil administratif de poursuivre dans la démarche entreprise. Rien n'interdit d'accepter la motion tout en demandant au Conseil administratif de conserver le cap. Elle réfléchit donc à la rédaction d'un amendement.

Une commissaire socialiste a compris que les documents qui avaient été remis à la commission par la DSIC étaient en quelque sorte une réponse aux questions

qui étaient posées par les commissaires. Elle ne voit donc pas comment elle pourrait voter cette motion alors même que la DSIC a pris, d'ores et déjà, toutes les dispositions nécessaires afin d'établir une véritable cartographie de la gestion des risques informatiques en Ville de Genève et ne voit donc aucune raison de soutenir cette motion.

Une commissaire motionnaire souligne que le document datant de février qui a été présenté n'aurait pas existé si la motion n'avait pas été déposée. Elle se pose donc la question de savoir si l'on peut considérer cet audit comme suffisant ou s'il convient au contraire de poursuivre cette démarche en en proposant d'autres par la suite.

Une commissaire du Parti démocrate-chrétien propose alors, avec quelques modifications successives suggérées par son collègue socialiste, l'amendement suivant: «Le Conseil municipal demande au Conseil administratif de poursuivre ses efforts en matière de gestion des risques informatiques, en particulier son analyse et son appréciation politiques.»

Une commissaire radicale considère que la commission a eu énormément de réponses. Elle s'estime donc pleinement rassurée et, à partir du moment où toutes les dispositions sont prises, elle juge qu'il faut par conséquent refuser cette motion afin de ne pas décourager le personnel de la DSIC. Elle poursuit en notant que le discours de la société privée auditionnée lui a donné l'impression d'une présentation à caractère commercial et qu'en contrepartie celui de M. Favre lui a semblé nettement plus authentique. C'est la raison pour laquelle elle lui accorde plus de crédit et que ceci la conduit à refuser la motion.

Un commissaire Vert affirme que son groupe ne soutiendra pas l'invite modifiée pour la raison que tout a été dit au cours des auditions au cours desquelles on a appris que des audits avaient lieu régulièrement et que le personnel était parfaitement connecté à la réalité. Il semble donc absolument clair que le nouveau poste dévolu à la sécurité va permettre de bien orchestrer cet ensemble de mesures et ne voit donc pas de motifs de soutenir cette motion amendée ou non.

Le président, faisant allusion au débat de la plénière, demande alors si compte tenu d'un certain nombre de données sensibles, il ne convient pas de demander le huis clos pendant la discussion.

Une commissaire pense que le huis clos pourrait avoir lieu si les documents confidentiels étaient remis à l'ensemble du Conseil municipal. Elle attire l'attention de la commission sur le fait que le rapport sera de toute façon publié et précise qu'il va de soi qu'un certain nombre de données confidentielles ne devront pas s'y trouver. L'ensemble de la commission partage alors l'avis de ne pas demander le huis clos.

Une commissaire propose donc formellement de voter son amendement qui prend la tournure suivante: «Le Conseil municipal demande au Conseil administratif d'améliorer sa gestion des risques informatiques tant du point de vue de l'analyse et de l'appréciation politique que de celui de l'établissement de procédures documentées.»

Le président met aux voix l'amendement, qui est refusé par 6 non (2 AGT, 3 Ve, 1 R) contre 4 oui (1 S, 1 L, 2 DC) et 2 abstentions (1 S, 1 UDC).

Le président met aux voix la motion M-772, qui est refusée par 7 non (2 AGT, 3 Ve, 1 S, 1 R) contre 2 oui (DC) et 3 abstentions (1 UDC, 1 L, 1 S).