GVA²
FONDATION POUR GENÈVE

11 juin 2024 - Dîner GVA2 sur la Cybersécurité – compte rendu

INTRODUCTION

Usurpation d'identité numérique, chantage, tentatives d'extorsion, hacking, phishing… que ce soit sur le darknet ou sur le clearweb, de plus en plus d'entités malintentionnées proposent leurs services criminels. Certaines d'entre elles disposent d'un service des ressources humaines et la plupart, d'un SAV chargé de négocier avec les victimes. Préoccupation majeure de nos sociétés connectées, la sécurité numérique est devenue une priorité tant sur le plan personnel que professionnel.

A Genève et en Suisse romande, de remarquables initiatives contribuent à renforcer la résilience numérique et à promouvoir un cyberespace plus sûr. Les représentants de trois d'entre elles nous ont fait l'honneur de venir présenter leurs activités qui contribuent à positionner notre région comme un leader mondial en matière de cybersécurité.

- **Monsieur Stéphane Duguin, directeur du Cyberpeace Institute** qui s'efforce de protéger gratuitement les plus vulnérables – hôpitaux, ONG humanitaires, etc. - contre les cyberattaques, d'analyser les menaces, de promouvoir la responsabilité des acteurs numériques, de militer pour la paix dans le cyberespace, pour la mise en place de normes éthiques et de mécanismes de réponse aux incidents cybernétiques grâce à des partenariats avec des organisations internationales, des gouvernements et des entreprises.
- **Directrice de la Trust Valley, Madame Lennig Pedron** nous parlé de cet écosystème unique qui réunit des acteurs de la cybersécurité, de la technologie et de l'innovation en Suisse romande. Ce réseau composé de collectivités publiques, institutions académiques et acteurs économiques, favorise l'échange d'expertise, la création de partenariats et le développement de projets innovants pour relever les défis de sécurité numérique auxquels font face les entreprises et les organisations de la région.
- Enfin, **Monsieur Raffael Maio, Chief Strategy Officer et co-fondateur de NetGuardians** nous a présenté les activités de cette société spécialisée dans la prévention de la fraude ainsi que la détection des comportements anormaux dans les transactions financières grâce à des solutions innovantes basées sur l'intelligence artificielle et l'analyse de données.

Pour compléter le tableau des compétences, nous avons également pu compter sur la participation du Capitaine de Police Patrick Ghion et de l'avocat spécialisé dans le droit digital, Me Nicolas Capt.

****

ALLOCUTIONS DES INTERVENANTS

Stéphane Duguin commence par insister sur le **coût humain ou parfois sociétal** que peut avoir une cyberattaque, bien plus coûteux que le coût financier. Il prend comme exemple une attaque survenue en Finlande en 2020 lors de laquelle une clinique psychiatrique a été la cible d'une cyberattaque de très bas niveau technologique. L'attaquant a pu récupérer l'intégralité des données de 30'000 patients (conversations intimes enregistrées en audio, vidéo ou

retranscrites) sans prendre la peine de les crypter. Après le refus de la clinique de répondre au chantage, il décide d'envoyer 31'000 mails de rançon aux patients en leur demandant de lui verser 500€ et en les menaçant de mettre leurs propos intimes sur le net. N'ayant pas pris la peine de sécuriser ces données, il est lui-même victime d'une attaque. Les données se retrouvent sur internet sans que personne ne puisse les en retirer.

L'**impact financier pour l'attaquant est assez faible** puisqu'il a gagné moins de 10'000 €. En revanche, les **impacts psychologique et sociétal sont sans aucune commune mesure**, pour une attaque où les victimes représentent 0.5% de la population. La Finlande a dû créer le plus grand service d'aide aux victimes de l'histoire du pays, plus de 25 000 plaintes ont été déposées, il y a eu des tentatives de suicide, des dépressions…

Protéger les protecteurs
Stéphane Duguin insiste sur la nécessité de protéger ceux dont le métier les confronte à la pédocriminalité en ligne ou la propagande terroriste et qui sont très affectés par les contenus violents auxquels ils sont exposés. Pour documenter et classifier ces contenus, ils sont contraints de visionner des contenus extrêmement violents des journées entières, engendrant stress, épuisement face à l'immensité ainsi que la complexité de la tâche. Stéphane Duguin a dû se battre avec l'administration d'Europol pour obtenir un soutien psychologique pour certains des fonctionnaires qui faisaient cela depuis plus de 15 ans. Le coût psychologique est un autre facteur expliquant la difficulté d'attirer des talents

Persistance des données volées
Aujourd'hui, en réponse à une cyberattaque, on répare les systèmes mais les données volées restent là où elles ont été mises par les criminels. Une énorme proportion sont revendues et tout un système de courtage très lucratif s'est mis en place. Ces données permettent aux criminels de faire des fiches d'identité pour faciliter leurs futures attaques. Dans d'autres domaines, on combat très activement le crime mais dans le cybercrime, il y a une partie non aboutie de la poursuite des auteurs car les données restent disponibles.

Contexte genevois
Grâce à des initiatives comme la Trust Valley, Genève et sa région, disposent d'un écosystème très actif qui tisse des liens forts entre les partenaires privés, la société civile, les entreprises, les diplomates, le monde de l'éducation ; tout cela permet d'attirer de nombreux talents et professionnels de la cybersécurité. Certaines conversations relatives à une législation mondiale comme les normes de comportement responsable dans le cyberespace ou un nouveau traité de combat contre la cybercriminalité, encouragé par la Fédération de Russie, ont déjà eu lieu à Genève.

CyberPeace Institute (CPI)
Pour lutter contre la cybercriminalité, le CPI, organisation à but non lucratif, offre gratuitement ses services à 280 ONG dont la sécurité est assurée par un réseau de volontaires. Ce système permet d'avoir une action de terrain, de répertorier les attaques comme ce qui s'est passé en Filande et d'avancer en termes de réglementation aux Nations Unies, dans l'Union européenne et ailleurs, pour que la loi aille à la même vitesse que les innovations criminelles.

Il est primordial d'avoir une législation pour combattre toutes les menaces cyber. C'est dans ce cadre qu'a été créée l'association féministe StopFisha, qui lutte contre le cybersexisme et les

cyberviolences sexistes et sexuelles. A la faveur du Covid, ce type d'attaque s'est multiplié de façon exponentielle avec des jeux macabres où on proposait à des internautes de donner l'identité et l'adresse sur des photos de femmes dénudées. Ce petit jeu est devenu très populaire avec un coût humain extrêmement violent.

Au-delà des attaques visant des systèmes avec des moyens très sophistiqués, une action sur la durée est nécessaire pour combattre celles qui impactent la vie des gens.

****

Lennig Pedron commence par relever le côté positif de la cybersécurité et souhaite souligner le **rôle primordial de ceux qui nous protègent**. Aujourd'hui les responsables de cybersécurité sont un peu seuls à supporter le poids des menaces qui pèsent sur les institutions. Les décideurs, conseils d'administration, de direction et autres top managers doivent également en prendre la mesure et assumer la responsabilité qui en découle.

La T**rust Valley** a été créée par les départements de l'économie des cantons de Vaud et de Genève pour coordonner les activités de l'EPFL, l'Université de Genève, de Lausanne, HEIG-VD, le Graduate Institute, le Cyberpeace Institute et des sociétés privées telles que NetGuardians dans le domaine. Un programme **d'accélération pour les startups** et **deux incubateurs ont été mis en place** pour permettre à des projets extrêmement jeunes de se développer tout en étant encadrés. Toutes ces entités forment un **écosystème de très haut niveau et mondial**.

Malgré la petite taille de notre pays et des moyens assez modestes, la Trust Valley a une grande agilité et un très gros potentiel de progression pour créer cette industrie au niveau national, permettre à des startups innovantes de voir le jour et aux nombreuses PME extrêmement innovantes de la région de grandir.

****

Raffael Maio - Scale-up issue d'un spin-off de l'Université du canton de Vaud, **NetGuardians** est une société qui compte une centaine de collaborateurs répartis dans 4 bureaux en Pologne, Singapour, Kenya et Romandie. Elle développe des logiciels pour prévenir la fraude et le blanchiment d'argent dans le domaine financier et bancaire. Leader en Suisse auprès des banques cantonales, la société compte également parmi ses quelques cent clients répartis dans une trentaine de pays, des banques privées ou des néobanques de toutes tailles.

Accélération de la digitalisation et de la menace
Au départ, NetGuardians concentrait ses activités sur la cybersécurité. En 2015, elle s'est recentrée sur la **prévention de la fraude** car à l'époque, celle-ci était marginale en Suisse. Depuis, l'environnement a énormément changé avec des menaces constantes.

Types d'arnaques
Depuis 2023, il y a une recrudescence des **Authorized push payments fraud** (APP fraud), pratiques qui consistent à inciter par la ruse un utilisateur à envoyer de l'argent sur un compte frauduleux. Dans 95% des cas, les personnes détentrices donnent volontairement leurs informations personnelles. Les 3 cas les plus fréquents dans ce qu'on appelle **l'ingénierie sociale** sont les **Support Scams,** surtout adressés à des personnes âgées qui pensent avoir

pour interlocuteur leur banque et se font dépouiller en donnant leurs codes d'accès. Ensuite les **Investment Scams** qui promettent des investissements très rémunérateurs et touchent principalement les 20-45 ans. Les **Romance Scams,** pratique qui consiste à faire croire à une relation amoureuse et qui vise à dépouiller la victime de ses biens. Enfin, **les fausses commandes et livraisons** sur Anibis, Ricardo et autre font également partie de ce type d'arnaque.

Social engineering et deepfakes
Les arnaques visant à manipuler les personnes à des fins d'escroquerie sont aujourd'hui facilitées grâce à l'IA qui assiste les criminels dans la rédaction de textes neutres, dépourvus de fautes d'orthographe ; ces erreurs permettaient jusqu'à maintenant de détecter ces pratiques. Les deepfakes audios indétectables sont aussi utilisées et contribuent à renforcer la menace.

Deepfakes et menaces sur la démocratie
Juste après l'invasion de l'Ukraine, une vidéo de Zelensky où il invitait ses soldats à déposer les armes a circulé. Une fausse vidéo de Joe Biden indiquant à ses concitoyens de ne pas voter à l'occasion de la primaire démocrate a également été générée par l'IA. Les **deepfakes audio** sont encore plus pernicieuses car il est difficile de repérer les éventuelles incohérences entre le son et l'image. Le phénomène existe depuis 2017 mais le premier règlement un peu ambitieux a vu le jour en Chine fin 2022. Selon une étude, d'ici 2 ans, 97% du contenu sur Internet sera synthétique tandis que la capacité technique à sa détection diminue en raison de l'IA générative. Cette technologie accessible à tous permet de mettre en doute la réalité de la preuve numérique et, pour un criminel, de nier être l'auteur d'un crime même s'il est filmé en plein acte. Du moment où les jurés auront un doute, cela lui profitera.

****

ETAT DES LIEUX

Ex d'attaques Hacking EMS – Impact sur la santé
Certains criminels s'en prennent à des hôpitaux ou des infrastructures critiques. Dans le cas des hôpitaux, la menace devient vitale dans le cas de patients atteints de graves pathologies. L'attaque de l'EMS de Vessy lui a fait perdre toutes ses données et notamment les posologies des patients. Dans un tel cas l'important est de réagir de manière transparente, non seulement à l'attention des patients et de leur famille mais également pour que cela serve à d'autres institutions qui sont la cible de hackers.

Infrastructures critiques
Même si le risque zéro n'existe pas, les infrastructures critiques, comme l'électricité, le transport ou la santé, bénéficient d'une **protection particulière** au niveau national. Pendant la période du Covid, 500 attaques sur des hôpitaux ont été répertoriées en 2 ans, sans que cela ne fasse grand bruit. Si des criminels rentraient dans un hôpital pour saccager les ordinateurs et menaient une attaque physique, cela ferait les gros titres. Si une cyberattaque est moins violente, la menace qu'elle fait peser sur son bon fonctionnement est tout aussi grave.

Le risque concernant les infrastructures critiques est très grand ; cela dit, il est très difficile (mais pas impossible) de les faire tomber en une seule attaque car elles sont gérées par une interconnexion de plusieurs systèmes. Le pire aujourd'hui, c'est que certains États comme la

Chine, se positionnent dans les infrastructures critiques en se préparant à attaquer. Sans passage à l'acte, cela ne tombe pas sous le coup du droit international.

Organisation des cybercriminels
Aujourd'hui, les groupes de cybercriminels fonctionnent comme de vraies sociétés : ils sont en concurrence les uns avec les autres et si l'un d'eux a un meilleur **service client,** il aura plus de chances d'être payé par la prochaine victime. Il y a de véritables SAV avec hotline pour « gérer la relation client » pour permettre aux victimes de récupérer leurs données.

Recrutement
La plupart de ces groupes sont pourvus d'un **service RH** chargé du recrutement aux quatre coins du globe, en se faisant passer pour une société de services informatique. C'est ainsi que procède la société ayant développé Conti, un des plus gros rançongiciel. En prenant leur poste, certains développeurs peuvent ne pas être au courant des activités criminelles de la société car le travail est très morcelé. S'ils peuvent, au début de leur contrat, ignorer la finalité de ses activités, cela devient rapidement impossible. Si certaines personnes restent, c'est forcément qu'elles s'en accommodent. Dans les équipes qui participent à des cyberattaques, les développeurs ne sont pas des tous criminels endurcis. En Birmanie, des informaticiens ont été enlevés et forcés à participer à des cyberattaques. Pour certains, c'est de l'argent facile mais si on ne leur propose pas de gagner leur vie honnêtement, le problème ne sera pas réglé. La cybercriminalité est un moyen d'améliorer son quotidien. Au même titre que la mafia, la traite d'êtres humains et le trafic de drogue, la **cybercriminalité est une nouvelle branche très lucrative de la criminalité, moins risquée et contre laquelle il est difficile de lutter.** Le côté lucratif accentue le problème.

A priori les dimensions de la cybercriminalité nous dépassent complètement. Les autorités disposent d'informations, non vérifiées mais plausibles, sur l'existence de **cybertowns** – des petites villes de 10 000 à 20 000 personnes - qui œuvrent dans la cybercriminalité.

Depuis 15 ans, cet **écosystème s'est professionnalisé dans l'interconnexion, la sous-traitance et le modèle de franchise**. En face, les méthodes d'enquête des pouvoir publics n'ont jamais réussi à s'adapter.

Réaction des victimes
Selon les statistiques de la Confédération, **aujourd'hui seuls 10% des cas sont rapportés**. **Se faire pirater reste encore très tabou**, souvent à cause du sentiment de honte d'avoir été berné. La **mise sous rançon,** est un des rares crimes où la victime est mise dans une posture mentale où elle a l'impression de participer au crime. Dès lors, il lui est très difficile, voire impossible de s'adresser aux forces de l'ordre.

Négociations avec l'attaquant
Les pirates demandent en général des sommes qui sont à la portée de leurs victimes et sont souvent prêts à négocier. Stéphane Duguin a conseillé une ONG rançonnée par un criminel qui, ayant lancé des attaques automatisées, n'avait pas conscience qu'il s'en était pris à une ONG s'occupant de la santé des enfants. En négociant avec la directrice, il s'est ému de ses activités et décide de faire un rabais sans pour autant renoncer à la rançon. Sur les conseils de Stéphane, la directrice temporise et le criminel a finalement abandonné.

Position officielle de la police
La position officielle est qu'il faut refuser de payer une rançon et une étude montre que les entreprises qui y consentent sont davantage sujettes à être réattaquées par la suite. Mais il y a parfois une **nécessité opérationnelle à payer la rançon pour permettre aux activités d'une société de reprendre** ; le coût du non-fonctionnement pouvant être plus élevé que celui de la rançon. Par ailleurs, le versement leur permet de récupérer des données. Les criminels ont quant à eux intérêt à ce que les victimes récupèrent leurs données pour que de potentielles futures victimes le sachent et en fassent de même.

Rapidité d'action vs besoins de l'enquête
À la suite d'une arnaque de type ingénierie sociale, il faut agir dans les 72 heures si on veut avoir une chance que la banque émettrice bloque les fonds. Dans ce laps de temps, on a des chances de récupérer l'argent mais pas de garantie. Au-delà, cela devient très compliqué car cela dépend du pays, de la banque ou de l'institut financier récepteur. Certains jouent plus ou moins le jeu. Malheureusement, l'action rapide peut aller à l'encontre des besoins d'une enquête policière qui, pour identifier les criminels, a intérêt à ce que l'argent parte vers sa destination finale. Dans les cas de blanchiment, les banques reçoivent l'ordre de ne pas bloquer les fonds pour faciliter l'enquête. Dès le mois de septembre, **« l'instant payment »** sera en place permettant le transfert instantané des fonds ; il sera dès lors impossible de les bloquer.

Risque de l'informatique quantique
Dans 8 à 10 ans, les ordinateurs quantiques seront capables de casser les méthodes de cryptographie utilisées actuellement. Le risque est de voir les données volées qui ont été cryptées, être décryptées dans 8 à 10 ans. Il faut donc protéger celles qui seront toujours sensibles dans 5 à 10 ans.

LIMITES DU DROIT

Classifier les attaques
Le CPI travaille sur une méthodologie visant à classifier les cyberattaques. Une attaque peut avoir de faibles conséquences financières mais un énorme coût humain. Les abus sexuels en ligne sur les enfants constituent les délits qui sont le plus durement punis. Toutes les innovations en termes de crypto et d'obfuscation de l'activité viennent de ce domaine-là. D'autres types de crimes sont bien moins punis et même si les attaquants sont identifiés, tous ne sont pas sanctionnés à cause des législations nationales. Si on prend l'exemple de l'attaque visant un EMS, le criminel, s'il était identifié, encourrait une peine de seulement 3 ans de prison.

Absence de législation internationale
Aujourd'hui, le travail des cybercriminels est facilité par l'absence de législation internationale. Les attaques réputationnelles sont facilitées par la multiplicité des supports et par la dimension internationale du problème. Les moyens de se défendre sont limités car il est très difficile d'envoyer des commissions rogatoires qui, pour la plupart, se voient opposer une fin de non entrée en matière. Pour ces cas, **l'attitude des plateformes est déterminante**. Si certaines réagissent bien et collaborent, d'autres s'abritent derrière une législation plus permissive comme c'est le cas en Irlande, siège de nombre d'entre elles.

Face à une attaque internationale, la Suisse ne peut rien faire au niveau légal. Aujourd'hui il n'existe que deux grands textes mais il s'agit seulement de recommandations de

comportement responsable dans le cyberespace. Un traité contre la cybercriminalité est en cours de négociation, poussé par la Russie et de nombreux États anti-démocratiques car il leur permettrait de criminaliser les comportements qui visent à garantir la liberté d'expression. Il ne vise évidemment pas à apporter de solution opérationnelle pour appréhender un cybercriminel.

Collaboration internationale
Récemment Lennig et Patrick étaient présents lors de discussions aux Etats-Unis où étaient présents Anthony Blinken et Joe Biden qui ont mis en avant le principe de **solidarité digitale** plutôt que de **souveraineté digitale**. Ils y ont annoncé des investissements en milliards de dollars mais aucun pays n'ayant la capacité de lutter seul, ils ont appelé à collaborer en écosystème, tout en préservant les intérêts des États. **Tout ce qui aide à la transmission rapide des données entre les États est le bienvenu.**

Enquêtes internationales
Grâce à la coopération d'États et de sociétés privées, de nombreux réseaux ont été démantelés et des enquêtes internationales se sont très bien déroulées. Récemment la Suisse a participé à une opération visant l'énorme société criminelle Lockbit. Ses activités ont pu être arrêtées pendant seulement 3-4 semaines mais cette organisation étant extrêmement tentaculaire, les responsables ont pu reprendre leurs activités en changeant de nom.

Environnement géopolitique
Au vu des tensions actuelles entre les États, la collaboration n'est pas toujours possible. Il est évident que la Russie, Chine ou la Corée du Nord, ne vont pas coopérer pour démanteler des réseaux criminels d'ampleur internationale. Au contraire, ces réseaux leur permettent de contourner les sanctions et de percevoir l'argent que les pays occidentaux ont parfois confisqué, comme c'est le cas pour la Russie

Identification des cybercriminels et répression
Les quelques cybercriminels ayant été identifiés proviennent en grande majorité de Russie ou d'Ukraine. Avant l'invasion, ils y étaient traités comme des criminels ; depuis, ils sont considérés comme des héros. Il sera très compliqué de les traduire en justice une fois la paix revenue, à moins qu'ils ne se trouvent sur une zone où il y a un accord d'extradition avec le pays qui enquête.

Lutte commune contre la cybercriminalité et la désinformation
Aujourd'hui, plus de **46% des attaques ciblent des États**, principalement des démocraties. Les acteurs de la lutte contre la cybercriminalité ont un rôle primordial à jouer sur la lutte contre la désinformation. Pour y faire face au niveau légal, on a deux modes opératoires pensés en silos : d'un côté les cyberattaques, malwares, l'intrusion dans les systèmes, etc., de l'autre, la désinformation. Un groupe criminel dispose souvent d'une infrastructure installée dans plusieurs pays qui n'ont pas de traités d'extradition. A partir de là, il peut véhiculer de la propagande terroriste, diffuser du contenu pédopornographique, de la désinformation et tout ce qui peut déséquilibrer un état démocratique. Face à ce type de menace, les pouvoirs publics, les services d'enquête, la société civile, sont organisés en silos ; certains travaillent sur la désinformation, d'autre sur les cyberattaques avec des organisations propres qui ne communiquent pas forcément entre elles. **Il est impératif de traiter contenu et le contenant de la même manière.**

Législation nationale
Dans de nombreux domaines, la Suisse a une stratégie attentiste qui consiste à voir ce qui se fait dans d'autres pays avant d'agir. En conséquence, sur certains sujets comme l'usurpation d'identité, nous sommes très en retard puisque nous punissons ce délit depuis septembre 2023, alors que la France s'est dotée d'une législation sur le sujet depuis 2010.

FORMATION

Pénurie de main d'œuvre
Pour NetGuardians, un des plus grands défis est la **pénurie de talents**. Chaque année, on dénombre environ 20'000 étudiants en informatique, soit 4 à 5'000 diplômés par an. Les domaines de l'informatique étant extrêmement vastes, les spécialistes en sécurité sont clairement insuffisants à combler la demande ce, à tel point que l'on est contraints d'importer des talents d'Espagne, de France ou du Portugal. La situation est très compétitive ce qui complexifie les processus de recrutement. C'est une des raisons pour lesquelles la société a ouvert des structures à l'étranger. Il est donc impératif de favoriser la filière si on souhaite former la relève car on estime que d'ici à 2030, la pénurie de personnel informatique sera d'environ 40'000 personnes.

Le cas de la police
Au sein de la police, un des principaux problèmes tient également à la **pénurie de main d'œuvre**. Alors qu'il faudrait pouvoir engager immédiatement les jeunes diplômés après leur cursus, ils doivent encore faire une année d'académie de police supplémentaire, plus une à deux années de stage. Lorsqu'ils arrivent enfin dans les services de cybersécurité, ils ont quatre années d'inactivité ce qui est dissuasif. De plus, au niveau salarial, les postes n'offrent pas les mêmes perspectives que dans le privé. Par contre, l'intérêt de venir à la police, tient au terrain de jeu qui est extrêmement intéressant. Pour contourner ce problème structurel, la police genevoise a mis en place des équipes mixtes composées de civils et de professionnels ; jusqu'en 2027, 4 civils par an vont rejoindre le service de lutte contre la cybercriminalité. Malheureusement, l'offre est plus importante que la demande. Il est nécessaire de faire savoir que la police recrute.

SOLUTIONS

Des solutions techniques limitées
Les sociétés sont vulnérables non pas à cause de leurs systèmes d'exploitation mais surtout à cause du facteur humain. Par les techniques du social engineering, un hackeur peut très facilement obtenir les codes d'accès d'un collaborateur. **C'est la raison pour laquelle il est important que les systèmes informatiques soient pourvus d'un double facteur d'authentification.**

La digitalisation de l'identité, une bonne idée ?
Sur cette question, les avis divergent parmi les experts présents car si cela simplifierait les démarches administratives, il est très difficile de garantir un système sans faille. Cela accroît par ailleurs le contrôle d'un État sur sa population. Par son attitude attentiste la Suisse semble vouloir se prémunir de toute restriction de leur liberté et d'atteinte à leur sécurité. Cela dit, il semble que cette évolution soit inéluctable même si le risque zéro n'existe pas.

Bitcoins et traçabilité
Il y a des moyens techniques qui permettent de contourner la traçabilité publique de la blockchain. Les groupes criminels savent comment faire pour récupérer des montants puis brouiller les pistes pour que leur origine soit impossible à retracer. Une des grosses problématiques tient à l'organisation par les Etats de plateformes d'échange entre les cryptos et la monnaie normale. Si elles n'existaient pas, les criminels n'utiliseraient plus de cryptos.

D'un point de vue infrastructure, il est impossible de lutter. On peut monter des murs aussi haut qu'on veut, le fait que tout est interconnecté nous rend vulnérable. Le seul moyen est de ne plus être sur internet. Le volet coopératif est le seul qui fonctionne.

EDUCATION

Inscrire une formation au numérique dans les programmes scolaires
Actuellement dans l'UE et en Suisse, il n'existe aucun cours sur le comportement numérique et le positionnement éthique. C'est également pour répondre à ce manque qu'on a créé le CPI afin d'envisager la formation de nos enfants à ces enjeux. Une formation a ainsi pu être "vendue" au DIP dans le cadre de la Semaine de la démocratie mais rien n'est encore inscrit au programme scolaire.

Signifier aux jeunes à l'importance de la vie privée
Il est nécessaire d'éduquer les jeunes générations à l'importance de la vie privée car ils n'ont aucune conscience de ce que c'est. Cela dit, avec le recul que l'on a maintenant et comme avec les enjeux écologiques, la jeune génération sera quand même amenée à mieux gérer son rapport à la technologie numérique. Lennig est un peu plus optimiste.

Faire de la prévention auprès des jeunes et des moins jeunes
Et finalement, un des axes de lutte c'est la prévention et pas seulement en organisant le mois du cyber mais en le faisant de manière bien plus régulière en martelant des messages de prévention. La police vaudoise est en avance là-dessus puisqu'elle créé des capsules vidéo sur les phénomènes cyber. Il faut donc s'organiser puisqu'elles puissent bénéficier à tout le pays.

Education
Il y a un manque d'éducation sur le numérique et sur toutes les menaces de cybersécurité dont personne ne parle à l'école. Il faut apprendre aux jeunes à remettre en question ce qu'ils voient sur internet et ce, dès le plus jeune âge, en même temps que leur présence sur internet et les réseaux sociaux.

FAVORISER L'EMERGENCE D'ECOSYSTEMES

Collaboration public-privé
Un des enjeux de la lutte contre la cybersécurité est lié à une meilleure collaboration public-privé. De nombreuses initiatives se créent mais leur évolution reste très lente en comparaison des cybercriminels qui eux travaillent très bien en réseau et se professionnalisent. Il faut que les pouvoirs publics collaborent pour mettre leurs forces en commun, en utilisant le cadre législatif existant en attendant qu'il évolue.

Cybersécurité de proximité, gratuite et garantie par les pouvoirs publics
Aujourd'hui, il y a un tabou à parler de cyberattaque, notamment au sein du conseil de sécurité des Nations Unies. On pourrait en effet créer une structure de gouvernance internationale à Genève mais il faut parer au plus urgent, penser à une cybersécurité de proximité qui s'adresse à chacun – entreprises et individus – et gratuitement sans attendre de grande agence internationale. **La cybersécurité devrait être un service public gratuit au même titre que la santé.**

Répliquer les modèles qui fonctionnent
Il faut miser sur les coopérations qui fonctionnent. Pour soutenir les ONG en cybersécurité gratuite, le CPI recrute des volontaires qui y dédient quelques heures par mois. Ce modèle est maintenant récupéré un peu partout dans le monde et il fonctionne assez bien. Il faut aller au-delà de la sidération face à un phénomène qui va trop vite, qui est trop gros, trop compliqué et face auquel, on pense qu'on ne peut pas lutter. Si on essaie de prendre le problème dans sa globalité, on n'y arrivera pas. Il faut donc essayer d'entreprendre des choses dont on peut mesurer l'impact.

POLITIQUE

Mener une politique ambitieuse
Aujourd'hui il y a de magnifiques initiatives, des écosystèmes faits de partenaires privés, d'initiatives émanant de la société civile et de formidables startups mais il manque l'ambition politique pour l'orienter dans la bonne direction avec une vision. **On a besoin d'une cybersécurité de proximité qui parle à tous les habitants et qui puisse offrir une sécurité gratuite**

Meilleure collaboration au niveau local
Il faut vraiment travailler en écosystème et pas juste deux cantons. Il faut un partenariat public-privé qui fonctionne et donc un investissement qui soit conséquent, qui permette de faire naître de l'innovation, aux académiques de former, de donner aux jeunes l'envie de rester ici pour disposer des compétences, voire de les importer.

Les politiques sont-ils armés pour comprendre ces enjeux ?
Les cantons de Vaud et Genève qu'on ne voit pas toujours travailler ensemble ont fait l'effort, grâce aux académiques de se mettre autour de la table. Et même si c'est à un niveau très local, une décision a été prise. Au niveau fédéral, l'infrastructure critique a été mise en place il y a un an tandis que dans d'autres pays cela fait 15 ans qu'elle l'est. Il y a un vrai besoin de **former les politiques qui le demandent car la législation numérique est très complexe**. Une multitude de lois qui impactent l'écosystème numérique existe mais si aucun moyen n'est investi pour les mettre en œuvre, elles ne servent à rien. La RGPD a eu un effet positif pour les entreprises en les protégeant légalement mais elle ne présente aucun avantage pour l'utilisateur qui clique aveuglement sur « j'accepte » sans être conscient de ce à quoi il consent. Il s'agit juste d'un transfert de responsabilité vers le citoyen. L'UE devrait faire pression sur les sociétés pour leur imposer un système qui protège le citoyen.

Structures policières compétentes
Au vu de ses particularités politique et linguistique, il est difficile de regrouper nos 26 cantons autour d'une seule structure. La police romande s'est regroupée autour du **Centre régional de**

compétences cyber pour la Suisse occidentale, directement issu de la stratégie nationale de protection de la Suisse contre les cyber-risques dont Patrick Ghion est le chef et qui est basé à Genève. Les ressources ne sont jamais suffisantes et serait inefficace de développer 26 structures de lutte. Mais le NEDIC dont il est le sous-directeur permet une coopération policière au niveau national. Il permet aux différentes polices spécialisées de Suisse de se retrouver une fois par mois pour avancer ensemble et organiser la coordination en faisant fi des barrières culturelles et linguistiques.