Berne, le 19 juin 2024

Poursuites pénales en matière de cybercriminalité. Efficacité des cantons

Rapport du Conseil fédéral donnant suite au postulat 22.3145, Andri Silberschmidt, 16 mars 2022 et 22.3017, Commission de la politique de sécurité du Conseil national, 15 février 2022

Table des matières

1 Introduction 4
1.1 Mandat politique 5
1.2 Contenu du rapport 6
1.3 Méthodologie 7
1.4 Définitions 8
2 Cybercriminalité en Suisse 9
2.1 Compétences et acteurs 9
2.2 Situation 13
2.3 Défis actuels 17
2.4 Conclusions 21
3 Résultat de la consultation 22
3.1 Bases légales 22
3.2 Organisation 22
3.3 Moyens techniques 27
3.4 Formation 28
3.5 Prévention 29
3.6 Mutualisation 30
4 Analyse des forces et faiblesses du système actuel 34
4.1 Forces 34
4.2 Meilleures pratiques 35
4.3 Faiblesses 36
5 Nécessité d'agir 37
6 Conclusions et prochaines étapes 40

Synthèse

Le Conseil fédéral publie le présent rapport donnant suite aux postulats 22.3145 Silberschmidt "Poursuites pénales en matière de cybercriminalité. Efficacité des cantons" et 22.3017 Commission de la politique de sécurité du Conseil national (CPS-N) "Renforcer les autorités de poursuite pénale dans le domaine des cryptomonnaies". fedpol et le Réseau national de sécurité (RNS) ont établi deux groupes d'accompagnement, l'un stratégique et l'autre technique, composés de représentants des autorités de poursuite pénale compétentes. Étant donné que le rapport porte principalement sur les activités des cantons en matière de lutte contre la cybercriminalité, fedpol a procédé à deux sondages pour recueillir les informations pertinentes.
Le rapport présente une vue d'ensemble de la lutte contre la cybercriminalité en Suisse, qui augmente constamment à la fois en termes de quantité de délits ainsi que de gravité des dommages causés. La très grande majorité des cantons s'est adaptée pour faire face à cette augmentation de la cybercriminalité. Ces adaptations portent sur la création d'unités dédiées à la lutte contre la cybercriminalité au sein des polices cantonales ainsi qu'à la création de postes de travail d'enquêteurs, de spécialistes forensiques TI ainsi que d'analystes. Ces créations de postes devraient se poursuivre les années à venir. La majorité des ministères publics disposent de procureurs entièrement ou partiellement spécialisés dans la lutte contre la cybercriminalité. Toutefois, de nombreux participants au sondage estiment que les effectifs actuellement dédiés à la lutte contre la cybercriminalité sont très insuffisants et ne permettent pas de traiter les plaintes reçues de manière approfondie. Le rapport recommande donc à chaque canton de procéder à une auto-évaluation afin de vérifier l'adéquation des moyens investis avec la situation en matière de cybercriminalité.

Deux entraves importantes à une amélioration de la lutte contre la cybercriminalité persistent: l'absence de bases légales permettant l'échange automatique d'informations de police entre les cantons et avec la Confédération, d'une part, et le régime de l'entraide internationale en matière pénale, relativement lent et non adapté aux preuves électroniques, d'autre part. En l'absence d'échange automatique d'informations de police, il est très compliqué de faire des liens entre des procédures menées dans différents cantons sur les mêmes auteurs. Cela induit un gaspillage de ressources et amenuise les chances de réussite des enquêtes. Cela empêche également le développement du renseignement criminel sur la cybercriminalité au niveau suisse. Or, celui-ci est capital lorsqu'il s'agit de mettre en place des mesures de prévention techniques ou de sensibilisation de la population, voire d'élaborer des stratégies cohérentes en matière de lutte contre la cybercriminalité. En son absence, il est également très compliqué de consolider des procédures concernant les mêmes auteurs, que cela soit au niveau cantonal ou fédéral. La Confédération est en train de combler cette faille via la mise en œuvre de la motion 18.3592 Eichenberger. Quant à l'entraide judiciaire internationale, elle peut constituer un défi pour les enquêtes. Ses limites (lenteur, droits de recours étendus, complexité administrative) peuvent être un avantage pour les cybercriminels et augmentent leurs chances d'échapper à la justice. Même lorsque les enquêtes aboutissent, il s'avère que de nombreux auteurs s'abritent dans des pays avec lesquels l'entraide judiciaire est très compliquée ou ne fonctionne pas. L'administration fédérale observe attentivement les évolutions internationales en la matière et évaluera prochainement les meilleures options.

La plupart des recommandations présentées dans ce rapport sont déjà évoquées dans le cadre de la Cyberstratégie nationale (CSN). En effet, les autorités de poursuite pénale avaient été étroitement associées à son élaboration. Par conséquent, les mécanismes d'implémentation prévus par la CSN – respectivement son comité de pilotage – sont pertinents pour assurer l'amélioration des conditions de lutte contre la cybercriminalité.

1 Introduction

Le présent rapport décrit les difficultés auxquelles se trouve confrontée la poursuite pénale suisse en matière de cyberinfractions et de criminalité numérique. Il fait suite aux postulats 22.3017 "Renforcer les autorités de poursuite pénale dans le domaine des cryptomonnaies" et 22.3145 "Poursuites pénales en matière de cybercrimnalité. Efficacité des cantons". En guise d'introduction, le cas suivant, qui a été anonymisé, illustre quelques-unes de ces difficultés.

Un jeune homme âgé d'environ 25 ans vit encore chez ses parents. Né à l'ère du numérique, il chatte avec des jeunes du monde entier sur différentes plates-formes de médias sociaux – souvent avec des arrière-pensées d'ordre sexuel. Il commence par entamer une relation d'amitié en ligne avec des jeunes âgés de 12 à 18 ans. Avec le temps, il les pousse à lui envoyer des photos osées, parfois pornographiques, d'eux-mêmes. Il enregistre les photos sur son disque dur. Dès qu'il a réuni suffisamment de photos compromettantes, il passe à l'offensive: il exige de l'argent et menace de publier les photos. Ce stratagème fonctionne dans de très nombreux cas, notamment parce que le jeune homme diffuse effectivement quelques photos sur Internet lorsqu'il n'obtient pas de paiement.

En procédant ainsi, ce jeune homme se livre à du chantage et utilise à cet effet des moyens numériques. L'acte en lui-même serait également possible sans moyens numériques, mais ceux-ci rendent la tâche nettement plus aisée. Dans ce type de cas, on parle de "criminalité numérique": il s'agit d'infractions qui, grâce à la numérisation, sont commises toujours plus facilement et plus rapidement, alors que la poursuite pénale est toujours soumise aux conditions-cadres fixées avant la numérisation à grande échelle. La "criminalité numérique" est donc différente du "cybercrime", qui désigne des infractions rendues possibles uniquement par des moyens numériques et qui visent des ordinateurs et des données, comme le font l'hameçonnage *(phishing)* ou les attaques de hackers.

Le jeune homme dissémine les photos sur différentes plates-formes. La communauté réagit: des utilisateurs indignés et dégoûtés signalent les contenus interdits aux exploitants de plates-formes Internet. Ceux-ci transmettent les signalements au *National Center for missing and exploited children* (NCMEC), en indiquant le compte d'utilisateur concerné. Le NCMEC procède au tri de ces signalements et en transmet les résultats aux interlocuteurs désignés dans chaque pays pour examiner les poursuites pénales à engager. En Suisse, il s'agit de fedpol, qui vérifie si les signalements entrants correspondent à un soupçon d'infraction selon la loi suisse et fait le constat suivant: les photos signalées sont de la pornographie interdite, parce que des personnes mineures y figurent. Dans le cas présent, il y a même plusieurs signalements que fedpol transmet à présent à la police cantonale concernée, parce que le jeune homme avait publié plusieurs photos. Les polices cantonales doivent toutefois donner la priorité à leurs cas et ne sont pas en mesure de s'occuper immédiatement de chaque signalement qui leur est fait. Durant des mois, le jeune homme continue donc d'exercer son chantage sur des mineurs, les poussant à produire de la pornographie interdite qu'il publie si ces derniers ne se montrent pas dociles. Le NCMEC envoie encore d'autres signalements.

fedpol examine également ces derniers et continue de les transmettre au canton compétent en matière de poursuite pénale. fedpol constate bien qu'il s'agit toujours du même auteur utilisant toujours le même modèle de photo, mais ne dispose pas d'une base légale pour entamer ses propres investigations. Le cas relève – comme la grande majorité des cas de criminalité numérique – de la compétence cantonale. La compétence fédérale n'entre en ligne de compte que pour les infractions extrêmement complexes et commises en série (par ex. attaques par rançongiciel et hameçonnage). Chacun de ces cas exige des ressources: des enquêteurs pour les auditions, perquisitions et rapports ainsi que des spécialistes TI et des analystes pour la sauvegarde des appareils, des données en ligne et des protocoles TI à analyser pour que l'administration des preuves ne comporte pas de faille. Le cas ne constitue toujours pas une priorité.

Or, voici que le jeune homme fait quelque chose qui le place par hasard au centre de l'attention de la poursuite pénale. Il part en vacances à l'étranger, où il poursuit ses agissements. Cela génère des signalements au NCMEC qui parviennent aux autorités de poursuite pénale de sa destination de vacances. Là encore, un certain temps s'écoule jusqu'à ce que la poursuite pénale soit ouverte. Finalement, les forces de l'ordre mènent une perquisition au lieu dont il était question dans les signalements au NCMEC et mettent en sûreté des données. Cependant, le jeune homme est de retour en Suisse depuis longtemps. C'est alors qu'une demande d'entraide judiciaire internationale adressée au canton compétent attire l'attention de la police cantonale concernée sur l'auteur de ces agissements et le cas remonte dans la liste des priorités. Des enquêteurs et des analystes se saisissent de l'affaire dont l'ampleur est à présent dévoilée au travers des enquêtes préalables menées par la police cantonale. Le ministère public cantonal ouvre lui aussi une procédure pénale à l'encontre du jeune homme en Suisse.

Les victimes du cas cité en exemple sont de jeunes personnes mineures du monde entier. Cependant, leur identification est indispensable pour l'administration des preuves. La coopération policière internationale est laborieuse, parce qu'il faut interroger tous les pays séparément et que les réponses se font parfois attendre ou ne viennent pas du tout. fedpol soutient la police cantonale dans ses multiples demandes aux autorités étrangères. Avec le temps, des victimes sont identifiées aux États-Unis, en Allemagne, au Royaume-Uni et en Norvège, mais la provenance des personnes dont l'identité n'a pas été établie reste incertaine.
En Suisse aussi, la coopération policière exige beaucoup de temps et d'efforts. Pour savoir si le jeune homme est apparu dans un contexte similaire auprès des autres polices cantonales, les enquêteurs doivent interroger chacun des 25 autres cantons séparément, étant donné que des obstacles d'ordre juridique et technique empêchent une demande automatique à toutes les polices cantonales.

La procédure pénale suit son cours et les agissements criminels du jeune homme sont interrompus. La procédure va toutefois encore durer un certain temps.

Ce cas illustre de manière exemplaire ce qui est développé dans le présent rapport: la criminalité numérique et les cyberinfractions soulèvent des difficultés liées à la compétence territoriale, à la coopération nationale et internationale, à la quantité croissante de signalements et de données et au besoin en ressources personnelles et techniques.

1.1 Mandat politique

1.1.1 Postulat 22.3017 "Renforcer les autorités de poursuite pénale dans le domaine des cryptomonnaies"

Le 8 juin 2022, le Conseil national a adopté le postulat 22.3017 de la CPS-N, intitulé "Renforcer les autorités de poursuite pénale dans le domaine des cryptomonnaies"[1]. La teneur du postulat est la suivante:

"Le Conseil fédéral est chargé d'examiner comment garantir que les autorités de poursuite pénale de la Confédération, en collaboration étroite avec les autorités cantonales, se dotent de la technologie nécessaire pour analyser les cryptomonnaies et suivre les transactions dans les systèmes blockchain, par exemple en cas de paiement d'une rançon ou d'autres fraudes utilisant ces technologies. Le rapport

[1] 22.3017 | Renforcer les autorités de poursuite pénale dans le domaine des cryptomonnaies | Objet | Le Parlement suisse (parlament.ch)

précisera également si les bases juridiques doivent être adaptées à cet effet et, dans l'affirmative, comment elles devraient l'être."

Le 27 avril 2022, le Conseil fédéral a proposé de rejeter le postulat, invoquant que le développement d'un centre d'analyse commun aux autorités de poursuite pénale fédérales et cantonales aurait pour conséquence un recrutement massif de personnel additionnel et que l'analyse des flux financiers de cryptomonnaies faisait déjà partie intégrante des enquêtes menées par les cantons ou par la Confédération. Il a ajouté qu'il appartenait aux autorités de poursuite pénale de développer leurs compétences dans ce domaine, une centralisation de celles-ci n'ayant de sens que si l'on envisageait de repenser tout le système de la poursuite pénale en Suisse. Il a souligné en outre qu'il existait déjà des services de coordination entre la Confédération et les cantons ainsi qu'entre les cantons.

1.1.2 Postulat 22.3145 "Poursuites pénales en matière de cybercriminalité. Efficacité des cantons"

Le 17 juin 2022, le Conseil national a adopté le postulat 22.3145 Silberschmidt Andri "Poursuites pénales en matière de cybercriminalité. Efficacité des cantons"[2]. La teneur du postulat est la suivante:

"Le Conseil fédéral est chargé d'établir, en collaboration avec le Réseau national de sécurité (RNS), un état des lieux sur les poursuites pénales menées par les cantons contre la cybercriminalité. Les résultats complets issus des analyses des différents cantons ne seront pas rendus publics. On publiera un rapport dont le contenu ne compromettra ni les tactiques des polices cantonales, ni la réputation des cantons."

Le postulat doit également vérifier si les cantons disposent des bases légales nécessaires à l'échange automatisé d'informations de police, si l'organisation des autorités de poursuite pénale a été adaptée et si des efforts de mutualisation des ressources sont nécessaires. Le 18 mai 2022, le Conseil fédéral proposait d'accepter le postulat, estimant qu'un état des lieux était indiqué notamment afin de permettre de compléter et d'optimiser le dispositif de lutte contre la cybercriminalité.

1.2 Contenu du rapport

Ce rapport a pour objectif de présenter l'état des lieux de la lutte contre la cybercriminalité en Suisse.
Pour ce faire, la méthodologie du projet est décrite au point 1.3 tandis que les définitions les plus importantes figurent au point 1.4.
Le chapitre 2 présente les acteurs impliqués dans la lutte contre la cybercriminalité en Suisse et leurs compétences. Par ailleurs, il dresse une analyse des différentes statistiques disponibles concernant la cybercriminalité, ce qui permet d'avoir un premier aperçu des tendances en la matière. Les principaux défis liés à la lutte contre la cybercriminalité sont également décrits.
Le chapitre 3 vise à répondre précisément aux questions des postulats et expose la manière dont les autorités de poursuite pénale se sont adaptées afin de faire face à la cybercriminalité. Différents domaines sont ainsi examinés, tels que la formation, l'organisation, les bases légales ou encore la mutualisation des ressources.
Le chapitre 4 vise à présenter les champs d'amélioration qui ont été identifiés via le sondage et pose les bases pour les domaines où il y a nécessité d'agir, qui figurent au chapitre 5. Les résultats principaux du rapport sont présentés au chapitre 6.

[2] 22.3145 | Poursuites pénales en matière de cybercriminalité. Efficacité des cantons | Objet | Le Parlement suisse (parlament.ch)

1.3 Méthodologie

La rédaction du rapport a été confiée au Département fédéral de justice et police (DFJP), respectivement à l'Office fédéral de la police (fedpol). Conformément au texte du postulat, fedpol a étroitement collaboré avec le RNS lors de tout le processus de rédaction du rapport. L'implication du RNS a permis d'avoir un interlocuteur neutre et d'assurer que les retours des acteurs cantonaux soient intégrés dans le rapport.
Le traçage des cryptomonnaies représente une part importante de la poursuite pénale en matière de cybercriminalité. Les difficultés qui y sont liées ne sont de loin pas les seules dans ce domaine, raison pour laquelle le présent rapport répond au postulat de la CPS-N.
Dans le contexte du présent rapport, les cryptoactifs sont définis ainsi: valeurs patrimoniales numériques (actifs virtuels), qui sont généralement représentées sur une blockchain. Ils se distinguent d'autres valeurs patrimoniales dans ce sens qu'il n'est possible d'en disposer qu'au moyen d'une procédure d'accès cryptographique, qui ne nécessite toutefois pas obligatoirement l'intervention d'un intermédiaire financier classique. En règle générale, un transfert implique l'utilisation d'une paire de clés, à savoir une clé privée (*private key*) qu'il faut garder secrète et une clé publique (*public key*)[3].
L'Autorité fédérale de surveillance des marchés financiers (FINMA) classe les actifs virtuels en trois catégories, à savoir les jetons de paiement, les jetons d'utilité et les jetons d'investissement, sachant qu'ils peuvent aussi se combiner dans des jetons dits hybrides. Du fait de leur caractère anonyme (au moins partiel), les jetons de paiement en particulier, ou même les cryptomonnaies, peuvent être utilisés abusivement à des fins criminelles et de blanchiment d'argent[4].

1.3.1 Modalités du rapport

Afin de remplir le mandat des postulats, les éléments suivants ont été mis en œuvre:

- Réalisation d'un sondage auprès des autorités suisses concernées. Le sondage a pour objectif d'établir l'état des lieux sur lequel est basé ce rapport et de permettre la création du benchmark. La quasi-totalité des polices cantonales et des ministères publics ainsi que 17 tribunaux cantonaux ont répondu au sondage dans son intégralité. Les chapitres 3 à 5 du présent rapport sont basés sur les données recueillies lors du sondage.
- Création de différents graphiques agrégeant les données quantitatives récoltées lors du sondage. Ces graphiques ont été distribués à la Conférence des commandantes et des commandants des polices cantonales de Suisse (CCPCS).

1.3.2 Organisation du projet

Le texte du postulat Silberschmidt demande explicitement à ce que le rapport soit rédigé en coordination avec le RNS. Concrètement, c'est fedpol qui a mené le projet tout en associant étroitement le RNS à chaque étape. Le mandat du RNS, validé par sa plate-forme politique, a été de coordonner l'implication des autorités cantonales concernées et de s'assurer que toutes les informations relatives à l'élaboration du rapport avaient été mises à leur disposition. La coordination a été assurée via l'établissement de plusieurs groupes de travail:

- Le groupe d'accompagnement stratégique, dirigé par le RNS, a assuré une implication et une information adéquates des acteurs compétents des cantons lors de l'élaboration du rapport. Le groupe d'accompagnement se compose comme suit: CCPCS, Prévention suisse de la criminalité (PSC), Conférence suisse des ministères publics (CMP), Association suisse des

[3] Fiche d'information- (Autorité fédérale de surveillance des marchés financiers FINMA, 2022)
[4] Le 28 février 2024, la deuxième analyse sectorielle du risque relatif aux actifs virtuels, du groupe de coordination de lutte contre le blanchiment d'argent et le financement du terrorisme (GCBF), a été publiée (ci-après rapport GCBF). Cryptomonnaies: risques accrus de blanchiment d'argent et de financement du terrorisme (admin.ch). Ce rapport fournit des indications supplémentaires au sujet des actifs virtuels et des fournisseurs d'actifs virtuels aux ch. 4.1 et 4.2.

magistrats de l'ordre judiciaire (SVR-ASM), Réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK), Office fédéral de la Cybersécurité (OFCS).

- Le groupe technique était dirigé par fedpol et se composait de spécialistes de la Confédération et des cantons. Il comptait des représentants du NEDIK, de la PSC, du Ministère public de la Confédération (MPC), d'un procureur cantonal, ainsi que de l'Association des chefs de police judiciaire suisses (ACPJS). Le groupe technique avait pour objectif d'assurer que l'expertise technique soit prise en compte lors des travaux et veillait à la collecte et à l'évaluation des informations nécessaires à l'élaboration du rapport.
- fedpol a également donné un mandat de conseil au Centre for Security Studies de l'École polytechnique fédérale de Zurich (EPFZ CSS). Le CSS a notamment soutenu fedpol en donnant des recommandations quant au rapport et en discutant des modalités de la représentation graphique des données.

1.4 Définitions

Dans le domaine de la cybercriminalité, il convient de distinguer entre les notions de cybersécurité et de cyberdéfense. La cybersécurité comprend l'ensemble des mesures ayant pour objectif la prévention, la gestion des incidents et l'augmentation de la résilience face aux cyberrisques. La cyberdéfense comprend quant à elle l'ensemble des mesures prises par les services de renseignement civils et l'armée et servant à protéger les systèmes sensibles dont dépend la défense nationale, à se défendre contre des attaques dans le cyberespace, à garantir la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace; enfin, ces mesures ont pour but de développer les capacités et les compétences de l'armée afin que celle-ci puisse apporter subsidiairement un appui aux autorités civiles.

Il n'existe pas de définition internationale de la cybercriminalité qui fasse l'unanimité. Selon les pays, la définition inclut différents délits. Dans les milieux académiques également, plusieurs classifications sont proposées[5]. Ce rapport se base sur la définition de la cybercriminalité qui figure dans la stratégie NEDIK 2022 – 2024[6]:

Cybercriminalité : Ensemble de tous les actes et infractions pénales dans le cyberespace. Comprend aussi bien la "criminalité numérique" que le "cybercrime".

➔ **Criminalité numérique -** Infractions qui étaient commises jusqu'à présent principalement dans le monde réel. En raison de la numérisation toujours plus importante, ces infractions classiques sont de plus en plus souvent commises à l'aide de moyens informatiques (qualifiées parfois de *cyber-enabled crimes*). Les phénomènes criminels typiques qui relèvent de la criminalité numérique sont par exemple la plupart des escroqueries réalisées tout ou en partie via Internet: les arnaques aux sentiments[7], l'arnaque au PDG ou au faux ordre de virement[8], les arnaques aux petites annonces[9] ou encore la fraude à l'investissement en ligne[10]. La criminalité numérique contient également les infractions de type pédocriminalité en ligne (partage de contenu pédocriminel, *grooming*[11], *live-distance child abuse*[12]) ainsi que les atteintes à la réputation. Ces infractions sont généralement

[5] (Wall, 2007)
[6] Cette définition est partagée par la très grande majorité des autorités de poursuite pénale suisses. Ainsi, 82 % des personnes ayant répondu au sondage mené dans le cadre de ce rapport ont indiqué utiliser cette définition. Certaines personnes ont indiqué utiliser également les dénominations des phénomènes cyber figurant dans le RIPOL. Ces phénomènes sont définis par le NEDIK en coordination avec l'Office fédéral de la statistique (OFS).
[7] Arnaques aussi appelées *romance scams*: établissement d'une prétendue relation amoureuse ou amicale pour ensuite exiger de l'argent (souvent sous prétexte de difficultés personnelles).
[8] Se faire passer pour un représentant d'une entreprise (président, employé, avocat) et inciter un partenaire commercial de l'entreprise ou un employé à verser de l'argent sur un compte inhabituel à l'étranger.
[9] Par ex.: les auteurs publient des annonces frauduleuses sur des sites en ligne. L'acheteur paie la marchandise, qui ne sera toutefois jamais livrée.
[10] Inciter quelqu'un à investir dans tel ou tel produit financier, celui-ci étant inexistant ou sans aucune valeur ou perspective de gains. Le commerce de ces produits (achat / vente) est simulé et n'a donc effectivement pas lieu.
[11] Le fait d'établir des contacts avec des enfants via Internet à des fins sexuelles, par exemple dans des forums de discussion ou sur les réseaux sociaux. Certains malfaiteurs visent une rencontre dans la vie réelle afin de se livrer à des actes sexuels avec la victime.
[12] Le fait de prendre part, via une webcam, à des actes d'ordre sexuel impliquant des enfants. Le consommateur / instigateur communique ses souhaits, par exemple via un forum de discussion, puis paie le montant demandé et visionne ensuite via une webcam les abus commis sur des mineurs.

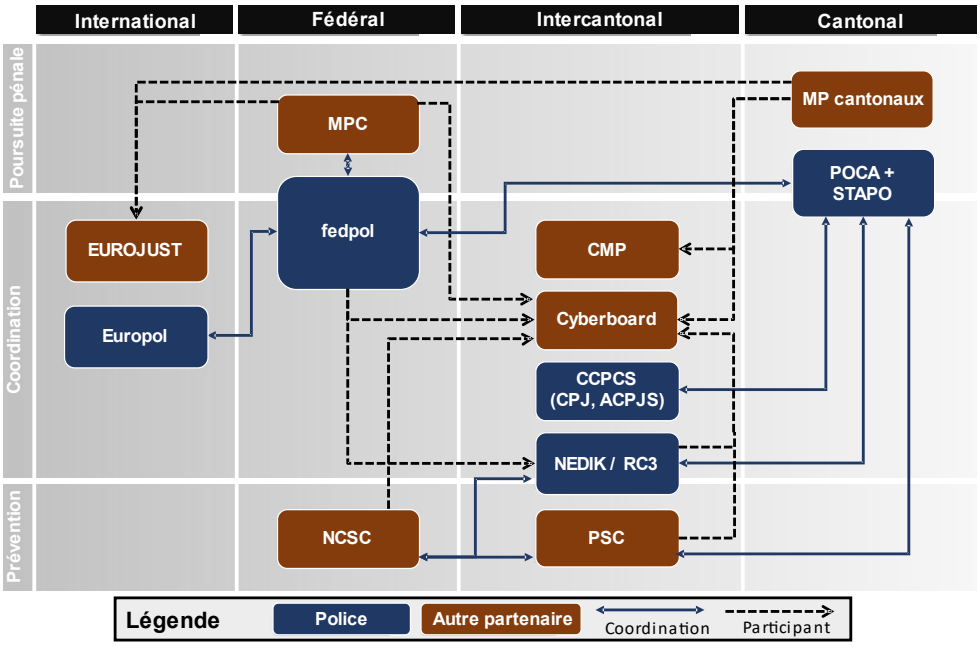
réprimées par des articles du code pénal (CP) qui s'appliquent autant aux infractions réalisées dans le monde réel que dans le monde virtuel.

➔ **Cybercrime -** Infractions de technologies avancées visant Internet, les systèmes de technologie de l'information ou leurs données, qui nécessitent également des technologies avancées d'enquête de la part des autorités de poursuite pénale (qualifiées parfois de *advanced cybercrimes* ou *hightech-crimes*). De manière générale, toutes les formes d'accès indus à des systèmes informatiques – ou *hacking* – sont considérées comme des cybercrimes, de même que les *ransomwares*[13] ou encore le *phishing*[14].

2 Cybercriminalité en Suisse

En Suisse, la compétence en matière de poursuite pénale de la cybercriminalité échoit principalement aux cantons, certains cas seulement relevant de la compétence fédérale. Toutefois, du fait du fédéralisme, de nombreux acteurs sont actifs dans la lutte contre la cybercriminalité. Ces acteurs et leurs compétences sont présentés au point 2.1. Le point 2.2 présente la situation de la cybercriminalité en Suisse. Cette appréciation est basée sur les statistiques policières de la criminalité, qui comportent une partie dédiée à la cybercriminalité depuis 2019. La lutte contre la cybercriminalité est rendue particulièrement ardue par toute une série de facteurs. Ces défis sont présentés au point 2.3.

2.1 Compétences et acteurs



Représentation des principaux acteurs et de leurs relations

[13] Un *ransomware* est un logiciel malveillant qui, une fois activé, chiffre les données de l'ordinateur ou du smartphone de la victime et requiert une somme d'argent pour les déverrouiller. Une autre version infecte et bloque l'ordinateur ou le smartphone (parfois aussi seulement le navigateur). Il envoie alors une notification apparemment officielle exigeant de la victime le paiement d'une amende en monnaie virtuelle, respectivement par le biais d'un moyen de paiement électronique, pour débloquer le système informatique.
[14] Rendre accessibles des données personnelles ou confidentielles de manière illicite.

2.1.1 Cantons

2.1.1.1 Polices cantonales

La poursuite pénale de la cybercriminalité est principalement la tâche des cantons, conformément à l'art. 22 ss du code de procédure pénale (CPP; RS *312.0*). Les cantons et les communes disposent de toutes les compétences requises pour identifier, empêcher et poursuivre les infractions pénales liées à la cybercriminalité qui relèvent de la police de sécurité et de la police judiciaire. À cet effet, les gouvernements cantonaux peuvent définir les infractions que la police doit poursuivre en priorité. Sur la base des lois de police cantonales, la police prend des mesures visant à empêcher ces infractions. En outre, les polices cantonales (et certaines polices municipales dotées d'une police judiciaire) sont chargées de mener les enquêtes engagées suite à leurs propres constatations ou à des dénonciations. Les constatations peuvent résulter de différents moyens, tandis que les plaintes sont le fait de particuliers. Par ailleurs, les polices cantonales traitent également les rapports transmis par fedpol, notamment en ce qui concerne la pédocriminalité ou les enquêtes préliminaires. Pour les cas dépassant les frontières cantonales ou nationales, elles peuvent compter sur le soutien du NEDIK et de fedpol.

2.1.1.2 Ministères publics cantonaux

Les ministères publics cantonaux traitent la majorité des cas de cybercriminalité, à l'exception de ceux qui relèvent de la compétence du MPC en vertu du CPP (art. 22 ss CPP). Les ministères publics cantonaux sont donc chargés de mener les poursuites pénales dans la très grande majorité des cas de cybercriminalité. Ils règlent ces affaires par le biais d'une mise en accusation ou d'une ordonnance pénale, d'une ordonnance de classement ou encore d'une décision de non-entrée en matière.
Afin de faciliter la coordination internationale, deux personnes sont détachées auprès d'Eurojust, plus précisément au sein de *l'European Judicial Cybercrime Network* (EJCN), où ils fonctionnent comme procureurs de liaison pour la Suisse[15].

2.1.2 Intercantonal

2.1.2.1 Conférence des commandantes et des commandants des polices cantonales de Suisse

La CCPCS promeut la collaboration ainsi que l'échange d'opinions et d'expériences entre les corps de police de Suisse. Elle dirige par ailleurs la réalisation opérationnelle des objectifs fixés au niveau politique pour toutes les questions importantes relevant de la police. La CCPCS dispose de plusieurs groupes de travail qui traitent de la cybercriminalité: le groupe de travail dédié à la formation cyber, la Commission de police judiciaire (CPJ)[16] ou encore l'ACPJS.

2.1.2.2 Réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique

La CCPCS a fondé le NEDIK en 2018. Ce réseau vise à concentrer les ressources spécialisées de manière à ce que la lutte contre la cybercriminalité puisse être menée de façon coordonnée et efficace ainsi que pour assurer le transfert des meilleures pratiques. Le NEDIK est composé d'un comité stratégique qui réunit les représentants des concordats de police et de fedpol ainsi que d'un comité opérationnel qui rassemble de manière bimensuelle des représentants de tous les cantons et de fedpol

[15] Depuis 2011, la Suisse collabore avec l'agence européenne Eurojust sur la base d'un accord de coopération en matière pénale. La Suisse dispose depuis 2015 de son propre bureau de liaison à La Haye, qui constitue un relais important entre les autorités de poursuite pénale suisses et celles des États membres de l'UE et des États tiers représentés au sein d'Eurojust. Le bureau de liaison fournit une assistance juridique et opérationnelle précieuse aux autorités de poursuite pénale suisses dans le cadre des demandes d'entraide judiciaire émanant de la Suisse et de l'étranger.
[16] La CPJ, qui se compose de représentants des cantons (quatre commandants de police en fonction et quatre membres de l'ACPJS) ainsi que d'une représentation de la Confédération (fedpol), a pour tâche de traiter de questions intercantonales en matière de police judiciaire.

afin d'assurer une coordination efficace des enquêtes. Outre la coordination opérationnelle, le NEDIK publie des bulletins mensuels dédiés à la situation de la cybercriminalité en Suisse, ainsi que, depuis 2022, des bulletins liés au phénomène de la fraude à l'investissement en ligne[17]. En quelques années, le NEDIK s'est affirmé comme l'acteur central en matière de coordination de la lutte contre la cybercriminalité en Suisse.

2.1.2.3 Prévention suisse de la criminalité

La PSC est un service intercantonal spécialisé dans les domaines de la prévention de la criminalité et de la promotion de la sûreté. Rattachée à la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP), la PSC est gérée par une commission permanente de la CCDJP, la Commission de direction de la PSC (dont fedpol est membre). La PSC a pour tâche de consolider la collaboration policière intercantonale dans le domaine de la prévention de la criminalité. La PSC a également pour tâche d'avertir la population, de lui expliquer les phénomènes qui se rapportent à la criminalité et les moyens de s'en prémunir et de trouver de l'aide. La PSC assure également la formation et la formation continue des membres de la police dans le domaine de la prévention de la criminalité et coopère étroitement avec l'Institut suisse de police (ISP). De par ses tâches, la PSC contribue régulièrement aux mesures prises par la police en matière de prévention de la cybercriminalité. La PSC représente les cantons au sein du RNS pour les questions de prévention de la criminalité. Elle est membre du Cyber-CASE ainsi que du comité élargi du NEDIK.

2.1.2.4 Centre régional de compétence Cyber pour la Suisse occidentale

Créé en 2019 sur proposition de la Conférence latine des commandants des polices cantonales (CLCPC), le *Cyber Competence Center* (RC3) romand est une plateforme de coordination qui vise à mutualiser les ressources et les compétences dans le domaine de la cybercriminalité. Il est piloté par les spécialistes de la police cantonale de Genève. Ses compétences sont liées à l'accès aux données numériques, à l'évolution dans le cyberespace, à l'exploitation dans l'Internet des objets (IOT)[18] et des véhicules ainsi qu'au processus d'exploitation et d'analyse du renseignement récolté. Le RC3 dispose d'un outil informatique en matière de renseignement cyber, nommé PICSEL (Plateforme d'Information de la Criminalité Sérielle En Ligne). Ce dispositif de renseignement permet notamment d'obtenir une vue globale de la cybercriminalité sur le plan romand et de favoriser la création et la gestion de séries de phénomènes.

2.1.2.5 Conférence suisse des ministères publics

La CMP[19] a pour but de promouvoir la coopération des autorités de poursuite pénale cantonales et fédérales. Elle encourage en particulier les échanges de vue réciproques entre les autorités de poursuite pénale cantonales ainsi qu'avec les autorités de poursuite pénale de la Confédération, de même que la coordination et le développement de leurs intérêts communs. Elle promeut l'unification des pratiques en matière de droit pénal et de procédure pénale. Elle prend position sur les projets législatifs de la Confédération, elle adopte des résolutions et des recommandations et elle prend part à la formation de l'opinion sur les questions relevant du droit pénal, de la procédure pénale et des domaines apparentés.

2.1.2.6 Cyberboard

La lutte contre la cybercriminalité constitue typiquement une tâche qui doit être menée conjointement par les autorités de poursuite pénale de la Confédération et des cantons. C'est pourquoi le concept du Cyberboard a été élaboré par le MPC en 2018, dans le but de renforcer la collaboration entre les

[17] Pour plus d'informations sur les prestations du NEDIK, voir le ch. 3.6.
[18] L'expression "Internet des objets" (Internet of Things, IdO) désigne des objets et appareils connectés à un réseau tel qu'Internet pour communiquer entre eux ou transmettre des informations. Sécurité de l'Internet des objets (admin.ch)
[19] https://www.ssk-cmp.ch/fr

autorités de poursuite pénale cantonales et fédérales, ainsi que la coordination dans le cadre du traitement conjoint des affaires intercantonales. Plate-forme fondée sur le maintien des structures et des compétences actuelles, le Cyberboard ne modifie pas les responsabilités et ne crée pas de nouvelles autorités.
Il se compose d'un échelon opérationnel composé de procureurs et de policiers ainsi que d'une représentation de l'OFCS et de la PSC[20]. Il dispose également d'un échelon stratégique, le Cyber-STRAT.

2.1.2.7 Institut Suisse de Police

L'ISP est une fondation de droit privé qui développe et met en œuvre, pour le compte de la police suisse, une stratégie de formation nationale. En assurant la coordination des contenus, des méthodes et de la didactique, l'ISP veille à la qualité et à l'unité de doctrine de la formation policière. Il garantit, dans un esprit de développement permanent, la cohérence de la formation de base – et sa pérennité dans la formation continue – ainsi que l'uniformité des examens fédéraux. En tant que centre national de formation, l'ISP organise la formation des cadres de police des niveaux I (sous-officiers) et II (sous-officiers supérieurs). Conjointement avec la Haute école Arc à Neuchâtel et la Haute école de Lucerne, il a créé un CAS (*Certificate of Advanced Studies*) pour la formation des officières et officiers (niveau III)[21].
Les deux autres grands axes de formation sont consacrés à la spécialisation professionnelle et à la formation des formateurs ou multiplicateurs. En matière de formation cyber, l'ISP a développé l'e-learning cybercriminalité (e-CC), qui est suivi par tous les aspirants policiers du pays. Par ailleurs, l'ISP offre également un cours de spécialisation (Cyber II). L'ISP se coordonne étroitement avec le groupe de travail dédié de la CCPCS.

2.1.3 Confédération

2.1.3.1 fedpol

En vertu de la loi du 7 octobre 1994 sur les offices centraux (LOC; RS *360*), fedpol assume, pour ce qui est de la lutte contre la cybercriminalité, les tâches d'office central, et fait, entre autres à ce titre, le lien entre l'étranger, lui-même et les corps de police cantonaux. fedpol assure l'échange d'informations de police criminelle avec Interpol et Europol, exploite le point de contact (SPOC) joignable vingt-quatre heures sur vingt-quatre et sept jours sur sept, selon la Convention de Budapest du Conseil de l'Europe, délègue un attaché de police spécialisé en cybercriminalité au bureau de liaison d'Europol et gère le point national de contact pour la coopération avec le NCMEC. fedpol décharge les cantons en triant les cas et en les attribuant directement au(x) canton(s) concerné(s), en maintenant la base de données nationale des valeurs de hash (NDHS), ainsi qu'en coordonnant, sur le plan opérationnel, les dossiers complexes nationaux et intercantonaux via le NEDIK. Pour toutes ces tâches, fedpol fait office de centre national de compétence en matière de cybercriminalité. fedpol représente en outre la Suisse dans divers groupes d'experts internationaux d'Europol et d'Interpol et, conjointement avec les spécialistes des grands corps de police cantonaux au sein du NEDIK, assure la diffusion de l'expertise et l'échange des meilleures pratiques. Dans le cadre des compétences fédérales (voir ch. 2.1.3.2 ci-dessous), fedpol mène également des enquêtes en matière de cybercriminalité sur mandat du MPC ainsi que de sa propre initiative (enquêtes de police). Il dispose pour ce faire d'un groupe d'enquêteurs cyber intégrés à la Division Criminalité économique.
Rattaché à fedpol, mais indépendant au niveau opérationnel en vertu des directives internationales, le Bureau de communication en matière de blanchiment d'argent (MROS) tient lieu de cellule suisse de renseignements financiers (*Financial Intelligence Unit,* FIU). Il réceptionne les communications de

[20] Il s'agit du Cyber-CASE, qui assure une vue d'ensemble nationale des affaires, le partage d'expériences entre cantons/autorités, les discussions au sujet d'affaires en cours, etc.
[21] CAS pour la Conduite des engagements de police à l'échelon d'officier – Haute école Arc (he-arc.ch)

soupçons des intermédiaires financiers, les analyse et demande si nécessaire des informations supplémentaires en Suisse ou à l'étranger. Si l'analyse débouche sur un soupçon initial d'infraction préalable au blanchiment d'argent prévue dans la législation ad hoc, de criminalité organisée ou de financement du terrorisme, il effectue une dénonciation à l'autorité de poursuite pénale compétente. Le MROS a pour autre tâche essentielle d'échanger des informations avec ses homologues internationaux. À cet égard, il est régulièrement confronté à l'utilisation frauduleuse de cryptomonnaies sur le plan national et international[22].

2.1.3.2 MPC

Le MPC est chargé d'enquêter sur les délits relevant de la juridiction fédérale, énumérés aux art. 23 et 24 CPP et dans des lois fédérales spéciales. Il lui incombe également de soutenir l'accusation dans ces mêmes cas. Une compétence facultative du MPC peut ainsi être retenue lorsqu'il s'agit d'un cas important de cybercriminalité ou de criminalité économique numérique, avec des soupçons d'infraction selon les titres 2 ou 11 CP, commis pour une large part à l'étranger ou dans plusieurs cantons sans prépondérance de l'un d'eux, les auteurs ayant agi depuis l'étranger en se protégeant au moyen de techniques d'anonymisation hors du commun et en usant de processus techniques particulièrement élaborés. Dans la pratique, le MPC enquête en particulier sur des séries de cas internationaux de *phishing*, de *malware* e-banking[23] et depuis peu, de *ransomware*. Concernant ce dernier phénomène, plusieurs procédures importantes ont été ouvertes par le MPC en 2022 et 2023.

2.1.3.3 OFCS

L'OFCS est le centre de compétence de la Confédération en matière de cybersécurité et le premier interlocuteur pour les milieux économiques, l'administration, les établissements d'enseignement et la population pour toute question relative à la cybersécurité. L'OFCS est responsable de la mise en œuvre de la Cyberstratégie Nationale (CSN)[24]. La CSN comporte plusieurs mesures spécifiquement dédiées à la lutte contre la cybercriminalité[25]. L'OFCS est également un partenaire important pour les autorités de poursuite pénale, dans la mesure où il dispose de capacités techniques de pointe et de plates-formes dédiées à la cybersécurité. Des échanges réguliers sur la situation en matière de cybercriminalité sont ainsi organisés entre l'OFCS et le NEDIK. L'OFCS dispose également d'une plate-forme d'annonce des cyberincidents, où la population peut signaler différents phénomènes cybercriminels[26]. Bien que cette plate-forme ne permette pas de déposer plainte, la population a l'option d'autoriser l'OFCS à transmettre les annonces aux autorités de poursuite pénale.

2.1.3.4 Office fédéral de la justice (OFJ)

Le Domaine de direction Entraide judiciaire internationale de l'OFJ est l'unité centrale de coopération internationale en matière de droit pénal pour la Suisse. Ce domaine est compétent pour les décisions concernant l'extradition, l'entraide judiciaire accessoire, le transfert de la poursuite pénale, la délégation de l'exécution de la peine et le transfèrement de personnes condamnées, également dans le domaine de la cybercriminalité.

2.2 Situation

La cybercriminalité se développe d'année en année et les cyberattaques sont en constante augmentation, suivant ainsi la numérisation de la société. Toutes ces connexions, faites pour des

[22] Cf. aussi rapport GCBF, ch. 7.2.1 ss.
[23] (Ministère public de la Confédération, 2022)
[24] (Conseil fédéral, 2023)
[25] Il s'agit des mesures "M12 Collaboration accrue des autorités de poursuite pénale", "M13 Vue d'ensemble des cas", "M14 Formation des autorités de poursuite pénale".
[26] OFCS Report (admin.ch)

raisons professionnelles, pour l'utilisation des réseaux sociaux ou encore pour faire du shopping en ligne, offrent des opportunités aux cybercriminels qui adaptent leurs stratégies pour commettre des infractions[27].

Bien que ce constat soit également effectué en Suisse, il n'existe pas de données statistiques sur ces dix à douze dernières années présentées de façon homogène pour mesurer l'évolution de la cybercriminalité. Les statistiques recueillies par l'Office fédéral de la statistique (OFS) représentent très probablement le meilleur indicateur de l'évolution de la cybercriminalité en Suisse, puisqu'il s'agit des plaintes déposées auprès des autorités de poursuite pénale. Une catégorie spécifique dédiée à la cybercriminalité n'existe toutefois que depuis 2019.

2.2.1 Statistiques policières de la criminalité[28]

L'OFS recense chaque année les infractions reportées par les autorités de police cantonales. Cependant, ces statistiques ne donnent qu'une vue partielle de la cybercriminalité, notamment car:

- les chiffres noirs de la cybercriminalité – soit les délits qui ne sont pas dénoncés – sont très élevés. Une estimation de la proportion de ces chiffres noirs est par définition très compliquée, toutefois il est généralement accepté que seuls 10 à 20 % des délits liés à la cybercriminalité sont dénoncés[29];
- les statistiques ne donnent pas d'information sur la suite judiciaire de chacune de ces infractions. Il n'existe pas de statistique sur le nombre de procédures ouvertes ou de leur issue;
- avant 2020, seuls les chiffres relatifs aux articles du CP étaient publiés dans les statistiques policières de la criminalité. Bien que certaines infractions figurant dans le CP aient une forte composante numérique, il reste très difficile d'évaluer la proportion des cas ayant une composante numérique ou non.

L'année 2020 aura servi de base de référence à la nouvelle méthodologie de comptabilisation des infractions ayant une composante numérique. Pour ce faire, la cybercriminalité est identifiée sur la base de la combinaison "Infraction – mode opératoire". Le mode opératoire ayant mené à l'infraction est choisi et constitue un phénomène qui sera comptabilisé dans les statistiques. Actuellement, le NEDIK répertorie un total de 33 modes opératoires distincts, lesquels sont ensuite répartis dans cinq domaines. Ces modes opératoires sont représentés dans le tableau ci-dessous:

Domaine	Cybercriminalité économique	Cyber-délits sexuels	Cyber-atteintes à la réputation et pratiques déloyales	Darknet et autres[30]
Nb MO	24	4	3	2
MO (criminalité numérique; cybercrime)	Phishing Hacking (2 types) Malwares (5 types) DDOS Cyber-escroqueries (12 types) Money/package mules Sextorsion (argent) Vol de cryptomonnaies	Pornographie interdite Grooming Sextorsion (sexe) Live Streaming	Cybersquatting Cyber-atteinte à la réputation (business) Cyberbullying/Cybermobbing	Commerce illégal sur le darknet Data leaking (fuite de données)

Tableau 1: Modes opératoires en matière de cybercriminalité

Les chiffres de 2019[31] à 2023 sont représentés à la figure 1 pour la totalité des cas recensés par l'OFS. Si l'on se réfère à ces chiffres, la cybercriminalité augmente de manière régulière depuis 2019, avec une augmentation d'environ 111 % en quatre ans. La grande majorité des cas relèvent de la criminalité

[27] (Khiralla, 2020)
[28] Toutes les données présentées dans ce chapitre proviennent des statistiques policières de la criminalité fournies par l'OFS.
[29] Crime Survey 2022, Communiqué de presse de la CCPCS du 24.8.2023: "Le taux de dénonciation des délits est très bas, puisque 90 % de ces derniers ne sont pas annoncés à la police. Il s'ensuit qu'une grande partie des cyberdélits restent dans l'ombre".
[30] Puisque le *darknet* ne représente qu'une infime partie des cas de cybercriminalité en Suisse, il a été ajouté au domaine "Autres" pour le présent rapport.
[31] Bien que les chiffres officiels n'aient été publiés que depuis l'année 2020, les chiffres de l'année 2019 étaient à notre disposition.

économique, soit plus de 80 % des cas chaque année. Les cyber-délits sexuels représentent le deuxième plus grand domaine, avec en moyenne environ 10 % des cas chaque année. Dans cette catégorie, la pornographie interdite représente environ 90 % des cas chaque année. Viennent ensuite les cyber-atteintes à la réputation et pratiques déloyales qui représentent en moyenne environ 5 % des cas chaque année. Finalement, les deux derniers domaines représentent ensemble à peine 0,1 % des cas chaque année.

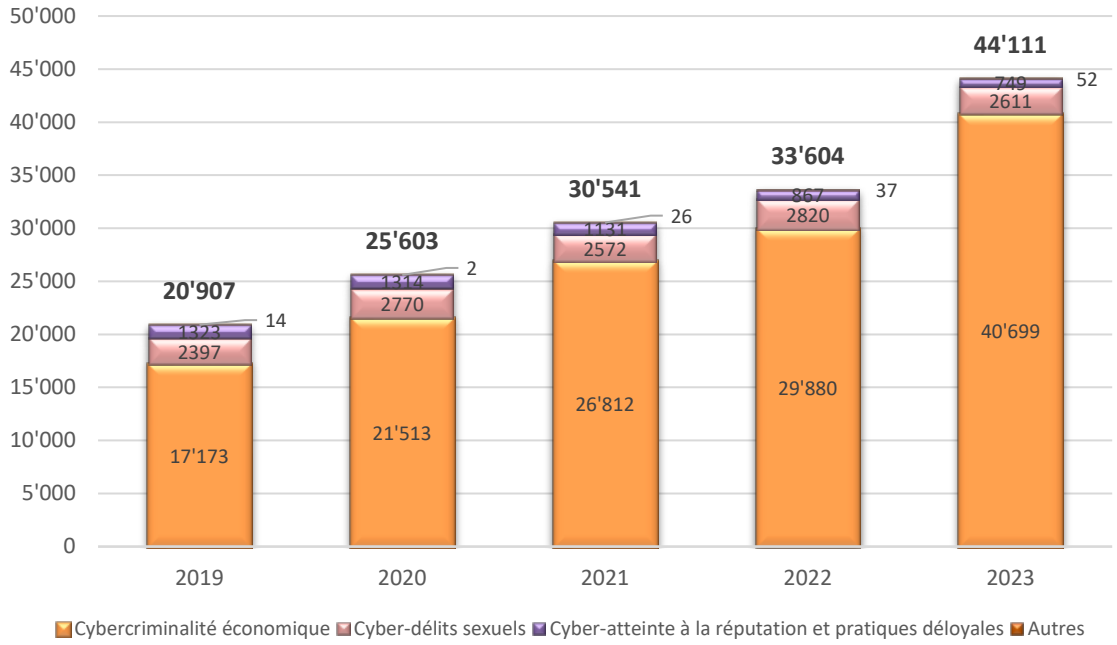


Figure 1: Nombre de cas annuels par domaine de cybercriminalité

L'évolution annuelle de chaque domaine de cybercriminalité est représentée à la figure 2. Ces variations sont fortement liées aux dépôts de plaintes. La cybercriminalité économique croît de manière régulière depuis 2019, avec une augmentation d'environ 137 % en quatre ans. Il s'agit du domaine connaissant la plus grande hausse. Les cyber-délits sexuels sont assez stables, avec environ 9 % de cas de plus qu'en 2019, et en légère baisse par rapport à 2020 et 2022. Quant aux cyber-atteintes à la réputation et pratiques déloyales, elles ont continuellement diminué en quatre ans, avec une baisse d'environ 43 %. Concernant les deux derniers domaines, il n'est pas pertinent d'apprécier leur évolution en raison du trop faible nombre de cas annuels.

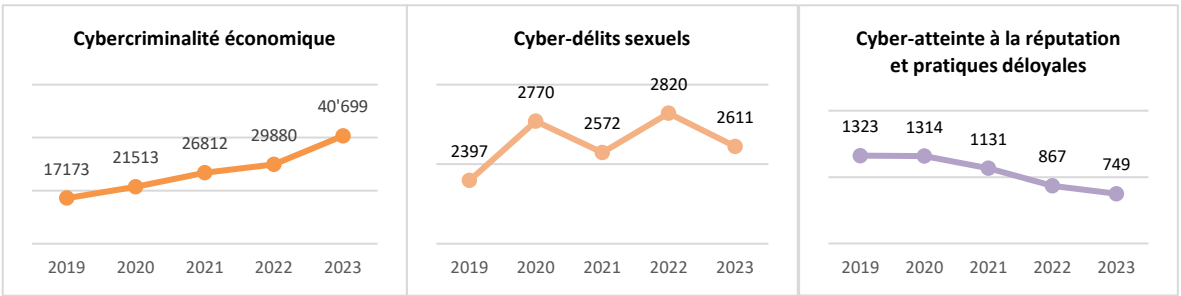


Figure 2: Évolution du nombre de cas annuels par domaine de cybercriminalité

La répartition du domaine de la cybercriminalité économique en sous-domaines est représentée à la figure 3. Parmi ceux-ci, les cyber-escroqueries[32] sont le sous-domaine le plus représenté, avec 75 à 80 % de cas de cybercriminalité économique. Si l'on prend en compte toute la cybercriminalité, alors deux tiers des cas environ relèvent des cyber-escroqueries. Les autres modes opératoires de

[32] La catégorie "cyber-escroquerie" agrège les données des douze modes opératoires suivants: CEO/BEC Fraud, magasins en ligne frauduleux, fausses annonces immobilières, fausses requêtes d'aide, fraude à la commission, arnaque au faux support technique, *romance scams*, petites annonces (objet vendu non payé), petites annonces (objet payé non livré), abus d'identité/de systèmes de paiement personnels pour commettre des fraudes, fraude à l'investissement en ligne, autre cyber-escroquerie. Les définitions de tous ces modes opératoires sont disponibles ici: Criminalité numérique | Office fédéral de la statistique (admin.ch)

cybercriminalité économique représentent, pour l'année 2023, un pourcentage de 9,3 % pour le *phishing*, 2,7 % pour le *hacking*, 1,2 % pour les *malwares*[33], 7,4 % pour les mules[34], 4,2 % pour les sextorsions (argent)[35] et 0,2 % pour les autres phénomènes.

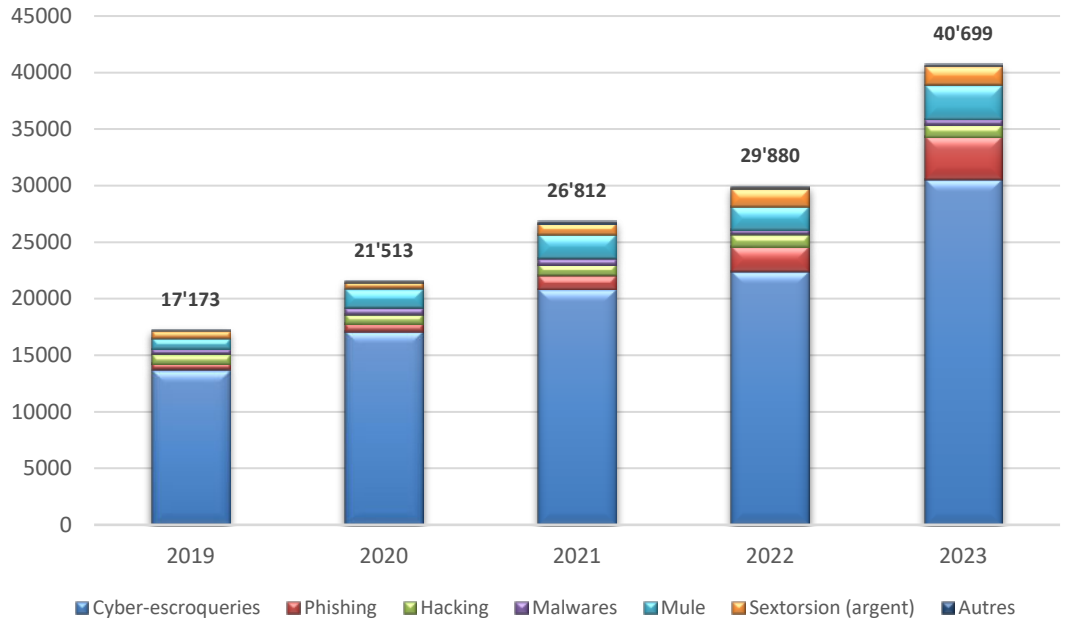
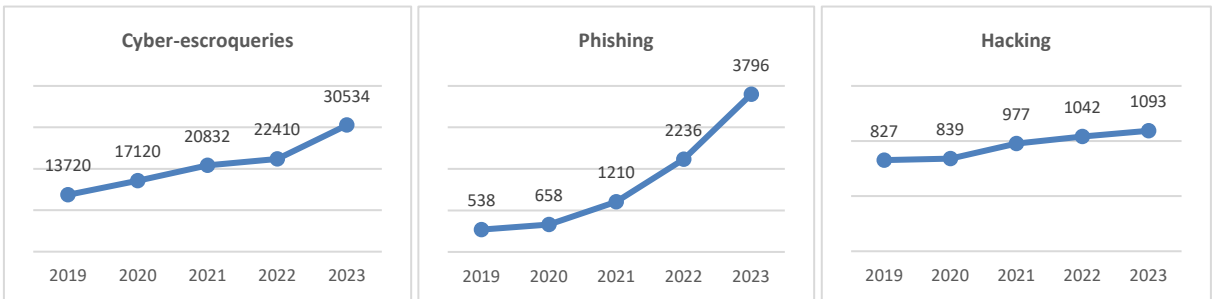


Figure 3: Répartition annuelle des cas de chaque sous-domaine de cybercriminalité économique

Concernant l'évolution de ces sous-domaines de cybercriminalité économique, elle est représentée à la figure 4. Les cyber-escroqueries ont augmenté de manière régulière entre 2019 et 2023, avec une hausse de plus de 123 % en quatre ans. Le phénomène de *phishing* a quant à lui également augmenté durant toute cette période, la hausse étant plus prononcée entre 2020 et 2023. Les cas ont augmenté de près de 605 % en trois ans. En ce qui concerne le phénomène de *hacking*, les cas ont plus légèrement augmenté durant la période sous revue avec une hausse d'environ 32,2 %. Les cas d'utilisation de *malwares* ont subi quelques légères variations dans les deux sens au fil des ans, mais les chiffres sont actuellement pratiquement similaires à ceux de 2019. Il faut noter que ces chiffres sont principalement liés à une diminution générale des modes opératoires autres que les *ransomwares*. En effet, ces derniers représentaient 46,5 % des cas de *malwares* en 2019 et plus de 70 % en 2022. Ils ont toutefois diminué pour atteindre 53 % en 2023. Finalement, les cas de mules ainsi que les cas de sextorsion (argent) ont assez fortement augmenté entre 2019 et 2023, la hausse étant respectivement de 227 % et 162,9 %.



[33] La catégorie *malwares* agrège les données des cinq modes opératoires suivants: *ransomware*, cheval de Troie e-banking, *spyware*, *rogueware/scareware, botnet*. Les définitions de tous ces modes opératoires sont disponibles ici: Criminalité numérique | Office fédéral de la statistique (admin.ch)

[34] Le fait de faire transférer de l'argent ou des marchandises d'origine criminelle par des tiers, pour la plupart recrutés sur Internet au travers de petites annonces de travail à temps partiel (personnes qui transfèrent de l'argent d'un pays à l'autre: *money mules* ; personnes qui acheminent des colis vers une autre destination: package mules).

[35] Action consistant à extorquer de l'argent à une personne au moyen de photos de nu ou de vidéos sur lesquelles la victime se masturbe et à la menacer de publier la vidéo sur *YouTube* ou de l'envoyer par exemple à ses amis sur *Facebook*.

Poursuites pénales en matière de cybercriminalité. Efficacité des cantons

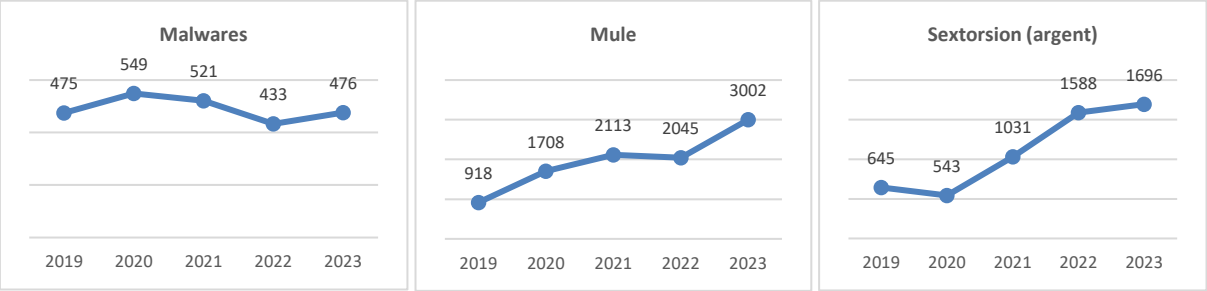


Figure 4: Évolution du nombre de cas annuels par sous-domaines de cybercriminalité économique

2.2.2 Analyse

La cybercriminalité a augmenté durant la période sous revue. Cette augmentation semble très forte depuis 2020. Cette hausse du nombre de cas s'est notamment concentrée sur les cyber-escroqueries, qui représentent désormais environ 70 % des cas recensés par l'OFS.

En plus d'une augmentation générale de la cybercriminalité selon les statistiques présentées ci-dessus, certains phénomènes cybercriminels constituent une menace toujours plus importante en Suisse, sans pour autant faire partie des modes opératoires les plus représentés.

C'est par exemple le cas des *ransomwares*, qui, bien que n'ayant pas aussi fortement augmenté que d'autres phénomènes ces dernières années, constituent actuellement la plus grave cybermenace pesant sur les organisations en Suisse; d'ailleurs, toutes les branches d'activité en font désormais les frais dans le monde entier. De même, cela nécessite un travail d'enquête très technique de la part des forces de l'ordre et des ressources suffisantes pour pouvoir mener de telles enquêtes.

Parmi les cyber-escroqueries, la fraude à l'investissement en ligne a pris de l'ampleur ces dernières années. Avec une augmentation d'environ 261 % entre 2020 et 2023 et une représentation de 8,4 % des cas de cyber-escroquerie, elle représente l'un des délits provoquant les pertes financières les plus importantes (plus de 100 millions de francs suisses pour l'année 2022).

Cette tendance générale de hausse de la cybercriminalité est également observée au niveau international. En effet, l'écosystème criminel numérique continue d'évoluer à un rythme alarmant. La numérisation affecte toutes les formes de criminalité et les méthodes utilisées par les cybercriminels sont de plus en plus souvent adoptées dans d'autres domaines de la criminalité[36]. De plus, plusieurs évolutions technologiques en cours sont susceptibles de modifier le paysage de la cybercriminalité. Certaines de ces évolutions ont déjà un impact visible, alors que d'autres en auront probablement un prochainement. Il s'agit par exemple de l'intelligence artificielle, de la technologie quantique ou encore des métavers[37].

2.3 Défis actuels

La lutte contre la cybercriminalité s'accompagne de défis particuliers: certains de ces défis sont d'ordre interne (ressources humaines et techniques dans les corps de police) et d'autres défis relèvent de tendances internationales, comme les différents régimes d'entraide internationale en matière pénale ou les évolutions technologiques qui bénéficient quasi toujours – en premier lieu – aux cybercriminels. Les défis présentés ci-dessous sont les plus importants: ils ont été sélectionnés par la consultation de la littérature ad hoc et suite aux discussions au sein des groupes d'accompagnement stratégiques et techniques.

[36] (European Union Agency for Law Enforcement Cooperation, 2021)
[37] (European Union Agency for Law Enforcement Cooperation, 2023)

2.3.1 Manque de moyens humains et techniques

- ❖ Le manque de ressources humaines est le principal problème dans la lutte contre la cybercriminalité. Le constat des spécialistes est sans appel: aucun corps de police en Suisse ne disposerait de suffisamment de ressources pour lutter efficacement contre la cybercriminalité.

Bien que la plupart des plaintes soient le plus souvent traitées, aucune enquête approfondie n'est menée (voir chap. 3.2.5). Les ressources sont très fortement mises sous pression, à la fois par la croissance continue de la cybercriminalité de masse (notamment les cyber-escroqueries) et par un nombre relativement stable de délits très complexes à résoudre (notamment les attaques de type *ransomware*). De par la masse de données croissante à traiter et la complexité technique du cybercrime, ce sont également les ressources de soutien aux enquêtes qui sont insuffisantes.

De nombreux corps de police ont du mal à trouver de nouvelles recrues. La Fédération suisse des fonctionnaires de police (FSFP) s'est ainsi inquiétée de cette situation à fin 2022[38]. Cette prise de position est à replacer dans le contexte des nombreux articles de presse évoquant cette problématique[39]. De multiples raisons sont évoquées pour justifier les difficultés de recrutement et les départs prématurés du personnel en poste: salaire insuffisant, conditions de travail exigeantes (horaire de nuit, peu de possibilités de travailler à temps partiel), critères de recrutements à revoir. En matière de lutte contre la cybercriminalité, la problématique est d'autant plus aiguë qu'il s'agit de former spécifiquement le personnel (par ex. via des cours dédiés de l'ISP) ou de recruter du personnel (analystes TI, analystes criminels) dont le profil est également très recherché par d'autres secteurs économiques[40].

Les autorités de poursuite pénale doivent disposer non seulement de personnel spécialement formé mais également d'outils facilitant l'identification des auteurs. Ces outils peuvent par exemple permettre de suivre les flux de cryptomonnaie[41] afin d'obtenir des informations sur le détenteur d'un *wallet*, par exemple la personne ayant reçu un paiement dans le cadre d'une affaire de fraude à l'investissement en ligne ou dans le cadre d'une attaque de type rançongiciel. Il s'agit également d'outils permettant de procéder à l'analyse des réseaux Internet ou encore de trier de larges quantités de données saisies. Ces outils sont généralement développés par des entreprises privées et sont onéreux. Par ailleurs, une multitude d'outils existent, certains offrant uniquement un nombre défini de fonctionnalités qui peuvent être rapidement obsolètes. Les autorités de poursuite pénale doivent donc régulièrement s'assurer qu'elles possèdent les outils les plus pertinents.

2.3.2 Absence de banque de données nationale

En Suisse, chaque police cantonale dispose de son propre système pour documenter ses enquêtes. Certaines banques de données fédérales sont communes (RIPOL[42], IPAS[43], KASEWARE CH[44]) et permettent de partager des informations sur les personnes et les enquêtes. Ces banques de données existent car elles sont fondées sur une base légale permettant aux cantons d'échanger des informations de police avec la Confédération et inversement (loi du 13 juin 2008 sur les systèmes d'information de

[38] Medienmitteilungen / Communiqués de presse : Fédération suisse des fonctionnaires de police FSFP (vspb.org)
[39] Die Kantonspolizei St. Gallen sucht verzweifelt nach Fachkräften - Blick ("La police cantonale saint-galloise recherche désespérément du personnel qualifié" – n'existe qu'en allemand)
Der Polizeiberuf im Aargau büsst an Attraktivität ein - aargauerzeitung.ch ("En Argovie, le métier de policier n'a plus la cote" – n'existe qu'en allemand)
Face à la pénurie de main-d'œuvre, les polices romandes peinent à susciter des vocations - rts.ch - Régions
[40] En 2030, il manquera près de 40 000 informaticiens en Suisse | ICTjournal
[41] 22.3017 | Renforcer les autorités de poursuite pénale dans le domaine des cryptomonnaies | Objet | Le Parlement suisse (parlament.ch)
[42] Le RIPOL est un système de recherches automatisées de personnes et d'objets. Il est exploité conjointement par les autorités compétentes de la Confédération et des cantons en vue de faciliter différentes tâches légales dans le domaine des recherches.
[43] IPAS est le système informatisé de gestion et d'indexation de dossiers et de personnes de fedpol. Il contient l'ensemble des communications échangées avec Interpol, ainsi que des données relatives aux affaires relevant des domaines suivants:
- service d'identification (en particulier les données personnelles relatives aux empreintes digitales et aux profils d'ADN);
- police administrative relevant de la compétence de fedpol.
[44] KasewareCH est le système d'enquête utilisé par fedpol, les polices cantonales, l'OFDF, le MPC et l'OFJ.

police de la Confédération [LSIP; RS *361*])[45]. Toutefois, la plupart des cantons **ne dispose pas des bases légales permettant l'échange automatique d'informations de police avec les autres cantons et la Confédération**[46]. Cela signifie que si l'auteur d'une infraction envoie une vague de mails de *phishing*, il est tout à fait possible que plusieurs cantons enquêtent en parallèle sur ce même auteur sans se coordonner. Pour régler ce problème, le DFJP travaille à la mise en œuvre de la motion 18.3592 Eichenberger[47]. Les cantons romands ont mis en place un outil afin de pallier cela, la plate-forme d'information sur la criminalité sérielle en ligne PICSEL[48]; bien qu'elle ait été rejointe par différents cantons depuis sa création, elle n'est toutefois utilisée que dans une minorité de polices cantonales.
En l'absence de base de données commune au niveau intercantonal ou national, la coordination de la lutte contre la cybercriminalité est compliquée. La mise en place du **NEDIK permet de limiter les doublons** en favorisant l'échange opérationnel sur les enquêtes en cours[49]. Au niveau des ministères publics, le **Cyberboard vise également à améliorer la coordination stratégique et opérationnelle** en matière de lutte contre la cybercriminalité[50]. Ce **but est difficilement atteignable en l'absence d'une banque de donnée nationale** qui permettrait d'avoir une vue d'ensemble des cas en cours de traitement. La coordination internationale souffre aussi de ce déficit, il est ainsi compliqué de s'engager dans une opération d'envergure internationale lorsque l'on n'a qu'une vue partielle des enquêtes en cours en Suisse.

> Les cantons romands ont mis en place un outil afin de pallier cela, la Plate-forme d'information sur la criminalité sérielle en ligne (PICSEL); bien qu'elle ait été rejointe par différents cantons depuis sa création, elle n'est toutefois utilisée que dans une minorité de polices cantonales. Pour régler ce problème, le Conseil fédéral travaille à la mise en œuvre de la motion 18.3592 Eichenberger.

2.3.3 Plaintes pénales trop rares

Dans 90 % des cas, les victimes des cybercriminels ne portent pas plainte. Cette réticence à porter plainte peut s'expliquer par différentes raisons: sentiment de honte d'avoir été victime d'une fraude, montant dérobé faible, procédures pour porter plainte compliquées ou encore doute quant au fait que les auteurs pourront être arrêtés ou les fonds récupérés. Ce très faible taux de plaintes pénales complique fortement le travail de la police. Il est ainsi très compliqué d'identifier un auteur prolifique et donc d'y dédier les ressources nécessaires lorsque seuls 10 % des délits sont dénoncés. La faible proportion du dépôt de plainte induit également que de nombreux auteurs ne seront tout simplement **pas poursuivis et jouissent ainsi d'une certaine impunité**[51].

> Le problème du dépôt de plainte sera partiellement résolu via la mise en œuvre du système de dépôt de plainte en ligne Suisse ePolice. Celui-ci permet de dénoncer de manière centralisée trois phénomènes de masse. Douze corps de police participent au dispositif; à terme tous les cantons y seront raccordés. La problématique du faible taux de dénonciation doit être considérée sous l'axe des ressources humaines. Ainsi, une augmentation de ce taux doit s'accompagner de la mise à disposition de ressources supplémentaires pour pouvoir enquêter.

[45] La LSIP règle notamment le réseau de systèmes d'information de police (art. 9 à 14), le système de recherches informatisées de police RIPOL (art. 15), la partie nationale du système d'information Schengen N-SIS (art 16), l'index national de police (art. 17) et le système de gestion des affaires et des documents de fedpol (art. 18).
[46] Motion 18.3592 | Échange de données de police au niveau national | Objet | Le Parlement suisse (parlament.ch)
[47] La motion demande au Conseil fédéral "de créer une base de données de police nationale et centralisée ou une plateforme reliant les bases de données de police cantonales existantes. Elle devra permettre aux corps de police cantonaux et aux organes de police fédérale de consulter directement, et depuis partout en Suisse, les données de police relatives aux personnes et à leurs antécédents. Si nécessaire, une base juridique devra être créée à cet effet". Le Conseil fédéral a accepté la motion et les travaux de mise en œuvre sont en cours.
[48] Communiqué de presse - Les polices romandes se dotent d'un Centre de compétence cyber | ge.ch
[49] Renforcement des efforts cantonaux contre la cybercriminalité et la pédocriminalité - KKJPD - CCDJP - CDDGP - FR
[50] (Ministère public de la Confédération, 2021)
[51] Das grosse Tabu der Cyberkriminalität: Erfolgreiche Erpresser (watson.ch; n'existe qu'en allemand)

2.3.4 Prévention encore insuffisante

Une fois l'infraction commise, il est généralement très compliqué d'attraper les auteurs. Les enquêtes sont longues et fastidieuses. Même lorsque les enquêteurs parviennent à identifier les auteurs, il est peu probable que les fonds soient récupérés ou que les auteurs soient finalement condamnés (notamment s'ils s'abritent dans des pays avec lesquels la coopération judiciaire est compliquée). De ce fait, la prévention est primordiale. Dans la plupart des cas, les infractions sont réalisables uniquement si la victime commet une erreur, comme avoir un mot de passe trop simple, ne pas vérifier la provenance des courriels, ne pas mettre à jour une application ou encore transférer des données sensibles à un inconnu. Il est donc important de sensibiliser la population à la mise en place de méthodes simples, efficaces et ne demandant pas trop d'efforts pour ne pas devenir victime de telles infractions. Les criminels adaptant constamment leurs arnaques aux développements technologiques et géopolitiques, il est important que la prévention fasse de même. Il s'agit également de vérifier dans quelle mesure les providers de services Internet peuvent augmenter leurs efforts en matière de prévention, notamment pour éviter le détournement de leurs plates-formes à des fins criminelles. À ce titre, l'échange entre les autorités de poursuite pénale et ces plates-formes est important car il permet la mise en place de mesures de prévention techniques.

2.3.5 Difficulté d'accès aux moyens de preuve électronique

De nos jours, dans le cadre de la grande majorité des investigations, les enquêteurs doivent avoir accès à des données électroniques, par exemple le contenu d'une boîte mail ou d'échanges réalisés par le biais d'applications de conversation en ligne. Dans le contexte de la cybercriminalité en particulier, l'obtention rapide de ces données est primordiale. En effet, les auteurs sont souvent aguerris et tentent d'effacer leurs traces au plus vite. Seulement, ces données ne sont que très rarement stockées en Suisse. La Convention de Budapest sur la cybercriminalité aborde déjà certains éléments à cet égard, mais se limite à la coopération avec les États parties et n'autorise l'accès direct et donc accéléré aux données de preuve que sur une base volontaire. Pour obtenir des données en dehors de ces possibilités, il faut par conséquent souvent recourir à l'entraide internationale en matière pénale traditionnelle. Cependant, l'entraide pénale traditionnelle est souvent trop lente pour permettre aux autorités de poursuite pénale d'effectuer leur travail de manière efficiente[52]. Dans de nombreux cas, elle n'est simplement pas accordée. Dans certains pays, les fournisseurs d'accès à Internet n'ont aucune obligation d'enregistrer le trafic de leur clientèle, de sorte que même si une demande fondée leur est transmise, ils ne pourront fournir aucune donnée. Et même s'ils possèdent ces données, les auteurs ont souvent la possibilité d'effacer leurs traces, étant donné la lenteur du processus. Certaines initiatives, à l'instar de la Convention de Budapest, établissent des instruments (*preservation request*) qui permettent de contourner partiellement les limites de l'entraide internationale en matière pénale. Toutefois, il n'existe pas d'harmonisation au niveau mondial et ces instruments ne donnent pas entièrement satisfaction[53]. Le 13 juin 2023, l'UE a adopté le paquet législatif e-evidence. Le but est de créer un cadre législatif cohérent dans le droit de l'UE afin de régler l'accès aux preuves électroniques et d'accélérer leur obtention[54]. Actuellement, le droit suisse se fonde uniquement sur l'entraide internationale en matière pénale, qui est relativement lente et n'est pas adaptée aux preuves électroniques[55]. Par conséquent, les grandes difficultés d'accès aux données électroniques représentent un très grand défi pour les autorités de poursuite pénale. Il est important que la Suisse suive les développements internationaux, en particulier au niveau de l'Union européenne, et qu'elle examine les mesures à prendre.

[52] (Office fédéral de la justice, 2021), p. 4
[53] (European Union Agency for Law Enforcement Cooperation, 2022)
[54] (Office fédéral de la justice, 2023), p. 3.
[55] (Office fédéral de la justice, 2023), p. 23.

2.3.6 Utilisation malveillante des nouvelles technologies

- De nombreuses technologies nouvelles sont rapidement utilisées à des fins néfastes par les cybercriminels. Que cela soit en matière d'anonymisation ou encore pour créer de nouvelles activités criminelles.

La numérisation de la société induit le stockage croissant de données critiques sous forme électronique. Les criminels ont rapidement saisi cette opportunité en développant et en déployant des rançongiciels. Les rançongiciels ne provoquent qu'une masse minime d'infractions de type cyber, toutefois ils causent des dégâts énormes[56] et difficilement quantifiables[57]. Les cryptomonnaies sont souvent utilisées dans de nombreuses escroqueries cyber, que cela soit comme moyen de paiement pour des rançons, comme véhicule pour blanchir des gains illégaux ou encore comme mécanisme de fraude propre[58]. Bien que les cryptomonnaies – contrairement à une idée répandue – soient généralement traçables, leur suivi nécessite le recours à du personnel qualifié et des logiciels onéreux[59]. D'autres technologies sont encore trop récentes pour être massivement adoptées par les criminels, toutefois l'intelligence artificielle a le potentiel d'être utilisée à de nombreuses fins criminelles: courriels de *phishing* convaincants, *malwares* adaptatifs, amélioration des conversations à des fins de pédocriminalité ou d'arnaque aux sentiments[60]. C'est également l'intelligence artificielle qui a permis l'émergence des *deepfakes,* soit des vidéos aux truquages hyperréalistes, qui peuvent être utilisées à des fins de pédocriminalité, de diffusion de fausses informations ou encore de fraudes[61]. Les univers de réalité virtuelle (ou métavers) peuvent aussi être utilisés pour la pratique de certaines activités criminelles également commises dans le monde réel, telles que le recrutement ou encore la pédocriminalité[62].

Les criminels peuvent de plus en plus facilement masquer leurs traces. De nombreuses applications facilement téléchargeables, et utilisées dans leur très grande majorité à des fins légales, permettent de crypter les communications. Certaines applications offrent également des prestations supplémentaires afin de garantir l'anonymat de leur clientèle. De la sorte, même lorsque ces entreprises sont sollicitées par la police – par l'intermédiaire du service SCPT – pour recevoir des informations, elles ne livrent que peu d'informations[63]. L'utilisation de ces techniques avec des technologies telles que les *Virtual Private Network* (VPN – qui permettent de masquer l'adresse IP) ou encore The Onion Router (TOR – qui garantit également l'anonymat) rend très compliquée, pour les autorités de poursuite pénale, l'identification des cybercriminels. D'autres techniques d'anonymisation, ou plutôt d'usurpation d'identité, permettent à des criminels d'imiter différentes informations identifiantes telles qu'un numéro de téléphone (*spoofing, smishing*) ou encore une adresse mail, voire un domaine Internet. Ces techniques sont utilisées dans de très nombreuses escroqueries, souvent de concert avec la technologie "*Voice Over IP*" ou les appels téléphoniques via Internet, qui permettent à la fois d'induire les victimes en erreur et de masquer les traces des auteurs[64].

2.4 Conclusions

La lutte contre la cybercriminalité est complexe. En Suisse, de très nombreux acteurs – en particulier les 26 polices cantonales et les 26 ministères publics cantonaux ainsi que le MPC et fedpol – sont impliqués dans cette lutte. Cette multitude d'acteurs complique la coordination. Il y est partiellement remédié par la création d'organes de coordination ad hoc. L'augmentation constante de la cybercriminalité s'accompagne d'autres défis pour les autorités de poursuite pénale: insuffisances des ressources humaines, cadre légal national et international parfois inadéquat, criminels agiles saisissant

[56] *Ransomware*: the number one cyber threat for enterprises... - NCSC.GOV.UK
[57] Dans de très nombreux cas, les victimes, généralement des entreprises mais également des entités publiques, renoncent à porter plainte et/ou payent la rançon. Au-delà du paiement de la rançon, il faut aussi prendre en compte les dégâts de réputation ainsi que les pertes liées au ralentissement, voire à l'arrêt total, de l'infrastructure.
[58] (European Union Agency for Law Enforcement Cooperation, 2021)
[59] Pour plus de détails à ce sujet, cf. rapport GBCF, ch. 7.4.1.
[60] (European Union Agency for Law Enforcement Cooperation, 2023)
[61] (European Union Agency for Law Enforcement Cooperation, 2022)
[62] (European Union Agency for Law Enforcement Cooperation, 2022)
[63] Internet_organised_crime_threat_assessment_iocta_2021.pdf (europa.eu) p. 9.
[64] FBI Warns Against Vishing Scams Over VoIP (securityintelligence.com)

les opportunités de chaque innovation technologique ou encore très faible taux de dénonciation des délits. Ces questions ont été évoquées dans la consultation menée auprès des autorités de poursuite pénale cantonales, dont les résultats sont présentés au chapitre 3.

3 Résultat de la consultation

Contrairement à ce qui a cours dans d'autres domaines comme la cybersécurité, il n'existe pas de standard international définissant ce qu'est l'efficacité en matière de lutte contre la cybercriminalité. Plutôt que de tenter d'établir l'efficacité des cantons, le rapport vise à répondre à la demande du postulant, respectivement à dresser un état des lieux de la lutte contre la cybercriminalité en Suisse. Le postulant demande notamment de vérifier si les bases légales et l'organisation ont été adaptées et s'il y a besoin de regrouper les ressources. L'état des lieux a été réalisé via un sondage qui comprenait des questions sur les bases légales, l'organisation (recrutement, créations d'unités dédiées) et la mutualisation. Pour avoir une vue complète de la situation, des questions concernant la formation, les moyens techniques, les meilleures pratiques et les mesures à prendre pour améliorer la lutte contre la cybercriminalité ont également été posées.

Au final, la quasi-totalité des polices cantonales et des ministères publics ont répondu au sondage ainsi qu'une majorité de tribunaux. Les réponses ont été discutées au sein des groupes d'accompagnement afin de contextualiser certains résultats. C'est la première fois qu'un sondage aussi vaste concernant la cybercriminalité est mené auprès des autorités de poursuite pénale suisses. L'excellent taux de réponse permet d'établir la vue d'ensemble requise par le postulat.

3.1 Bases légales

- Seule une minorité de cantons dispose des bases légales requises pour procéder à l'échange intercantonal automatique d'informations de police. Une majorité de cantons dispose des bases légales pour effectuer des mesures préventives secrètes sur Internet.

Seule une minorité de polices cantonales (11) a indiqué disposer des bases légales permettant un échange intercantonal automatique d'informations de police qui soit complet. Quatorze polices cantonales ont indiqué disposer des bases légales permettant un échange partiel (soit généralement l'échange au cas par cas). Trois cantons sont en train d'adapter leurs lois cantonales afin de permettre l'échange automatique de données.

La très grande majorité des polices cantonales (23) dispose des bases légales permettant d'effectuer des mesures préventives secrètes sur Internet, y compris le monitoring de réseaux pair-à-pair ou l'utilisation d'identités d'emprunt (pseudonymes) sur Internet. De plus, deux polices cantonales ont indiqué que l'adaptation des bases légales était en cours. Bien que la majorité des cantons dispose des bases légales, cela ne signifie pas pour autant qu'elle dispose des moyens techniques ou humains pour effectuer de telles mesures.

3.2 Organisation

Les très nombreux corps de police suisses disposent chacun d'une organisation qui leur est propre. Des facteurs démographiques et économiques différents induisent un nombre de (cyber)délits très variable

d'un canton à l'autre[65]. Par conséquent, il est très difficile de comparer des chiffres tels que la taille des polices judiciaires ou des unités dédiées à la lutte contre la cybercriminalité. Il n'est pas facile, même pour chaque police au niveau individuel, de quantifier combien de ressource sont dédiées à la lutte contre la cybercriminalité (voir encadré ci-dessous sur la notion de "cyber-enquêteur"). En-effet, le traitement d'une plainte liée à la cybercriminalité implique de nombreuses étapes qui ne sont pas toutes effectuées par les "cyber-enquêteurs". Le recueil de plaintes, l'analyse forensique, les mesures secrètes sont toutes effectuées par d'autres spécialistes. De même, les spécialistes cyber – du fait de la numérisation de la société – sont amenés à aider leurs collègues dans toutes sortes de procédures qui ne sont pas forcément liées à la cybercriminalité. Certains corps de police traitent un volume de cas si faible qu'ils n'ont pas besoin d'avoir un poste dédié à plein temps à ce type d'enquêtes. Il existe également plusieurs cantons qui disposent d'un accord pour bénéficier des prestations TI forensiques d'un autre canton: par conséquent, ces cantons ne disposent pas de leurs propres ressources en matière d'informatique forensique.
Du fait de tous ces facteurs, les chiffres présentés dans ce sous-chapitre ont généralement été consolidés au niveau suisse. Afin que les données soient les plus fines possibles, il est recommandé à chaque canton d'établir un état des lieux – au niveau individuel – des moyens dédiés à la lutte contre la cybercriminalité.

3.2.1 Structure

En matière de lutte contre la cybercriminalité, plusieurs formes d'organisation existent. De nombreuses polices optent pour la création d'une unité dédiée d'enquêteurs cyber. Cette unité ne s'occupe que de la cybercriminalité. Certaines unités s'occupent exclusivement du cybercrime tandis que d'autres s'occupent également de la criminalité numérique. Dans la plupart des polices, des enquêteurs qui ne font pas partie de ces unités enquêtent également sur la cybercriminalité (généralement la criminalité numérique). Par ailleurs, tous ces enquêteurs sont soutenus par des analystes criminels et des spécialistes forensiques TI. Ceux-ci fournissent la plupart du temps des prestations pour l'ensemble de leur corps de police judiciaire. Par ailleurs, certaines polices ont mis en place un réseau de points de contact cyber dans les unités décentralisées.

3.2.2 Unité cyber dédiée

De manière générale, la très grande majorité des polices cantonales (22 / 26) a prévu de créer ou a créé une unité d'enquêteurs exclusivement dédiée à la lutte contre la cybercriminalité. La taille de ces unités varie fortement d'un canton à l'autre. Selon les retours des cantons, il est ainsi prévu que ces unités soient composées de 190 emplois à temps plein (ETP) pour toute la Suisse.

> La définition d'un cyber-enquêteur varie grandement d'un corps de police à l'autre: dans certains corps, le cyber-enquêteur va reprendre majoritairement des enquêtes liées au cybercrime, dans d'autres, ce sera plutôt des enquêtes liées à la criminalité numérique et dans d'autres encore, les cyber-enquêteurs constitueront un pool de soutien qui épaulera les collaborateurs dans toutes les enquêtes ayant une composante numérique. Il est donc très difficile de quantifier précisément combien de cyber-enquêteurs sont présents dans chaque corps. De plus, il y a des corps dont le volume de cas de cybercriminalité est si réduit qu'il ne justifie pas forcément la création d'un poste à plein temps.

[65] En Suisse, on compte ainsi en moyenne 3,6 délits / 1000 habitants. Il y a toutefois de grandes variations selon les cantons. Neuf cantons annoncent ainsi plus de 4 délits / 1000 habitants (maximum = 6,11 / 1000) et 6 cantons annoncent moins de 3 délits / 1000 habitants (minimum = 0,96 / 1000).

3.2.3 Création de postes

- ❖ Une majorité de polices cantonales disposent d'une unité dédiée à la lutte contre la cybercriminalité. Elles ont également renforcé leurs effectifs afin de lutter contre la cybercriminalité et prévoient de continuer à engager du personnel supplémentaire ces dix prochaines années.

Selon le retour des cantons, plus de 167 postes de cyber-enquêteurs et de spécialistes forensiques TI ont été créés au sein de 23 polices cantonales durant ces dix dernières années. Au niveau des cyber-enquêteurs, environ 85 postes ont été créés dans l'ensemble de la Suisse ces dix dernières années. Ces postes supplémentaires sont répartis dans 23 cantons. Au total, ce sont plus de 82 postes supplémentaires de spécialistes forensiques TI qui ont été créés dans 23 polices cantonales différentes.

Les cyber-enquêteurs sont soutenus par d'autres spécialistes, par exemple des experts en forensique TI. Ces experts ont de nombreuses missions: sécurisation des moyens de preuve TI (disques durs, téléphones, objets connectés), analyse de leur contenu, analyse des réseaux, des flux de cryptomonnaie. Du fait de la numérisation de la société, ces experts sont actifs dans quasi toutes les enquêtes et pas uniquement dans les enquêtes liées à la cybercriminalité. Par ailleurs, d'autres unités (par ex. liées à des mesures secrètes comme l'infiltration en ligne ou l'observation ou encore dédiées à l'analyse criminelle opérationnelle ou tactique) sont également impliquées dans ces enquêtes.

Selon les retours des cantons, 142 postes supplémentaires d'enquêteurs et de spécialistes forensiques TI seront créés dans 21 cantons différents ces dix prochaines années. Ces efforts supplémentaires correspondent à la création de plus de 87 nouveaux postes d'enquêteurs cyber dans 21 polices cantonales différentes. Quinze cantons vont également renforcer leurs effectifs de spécialistes forensiques TI pour un total de 55 postes supplémentaires.

Au niveau régional, l'augmentation en chiffres absolus varie grandement d'un concordat de police à l'autre. Le concordat PKNW[66] enregistre la plus forte hausse d'effectifs (+113 enquêteurs et spécialistes forensiques TI). Le concordat CLCPC[67] va presque tripler les effectifs supplémentaires dédiés à la lutte contre la cybercriminalité ces dix prochaines années (+55,5 ETP contre +30 ces dix dernières années). De manière générale, à l'échelle des concordats, des efforts ont été consentis ces dix dernières années et seront maintenus ces dix prochaines années.

En comparant le nombre de création de postes d'enquêteurs au nombre de délits cyber enregistrés en 2022, on arrive à un ratio relativement stable entre les différents concordats: il varie entre 133 délits / nouveau poste d'enquêteur (PKNW) à 201 délits / nouveau poste d'enquêteur (CLCPC). Si l'on compare le nombre de délits cyber par concordat au nombre total de création de postes (enquêteurs +

[66] Le *Polizeikonkordat Nordwestschweiz* (PKNW) regroupe les polices cantonales d'Argovie, de Bâle-Campagne, de Bâle-Ville, de Berne et de Soleure.
[67] La Conférence latine des commandants des polices cantonales (CLCPC) regroupe les polices cantonales de Fribourg, de Genève, du Jura, de Neuchâtel, de Vaud et du Valais.

spécialistes forensiques TI), les résultats sont encore plus stables. Ils se situent entre 85 délits / nouveau poste d'enquêteur (PKNW) à 95,9 délits / nouveau poste d'enquêteur (Ostpol[68]).

Et au niveau fédéral? Les ressources de fedpol pour lutter contre la cybercriminalité n'ont pas été augmentées au cours de la dernière décennie. Depuis 2020, fedpol mène environ une dizaine de procédures par année liées à la cybercriminalité. Ce sont ainsi des enquêteurs cyber, prélevés sur l'effectif global de la Division Criminalité économique, qui sont affectés à ces enquêtes, au détriment donc d'autres mandats du MPC. Suite à l'adoption, le 28 février 2024, par le Conseil national du postulat 23.4349, un examen des ressources de fedpol, y compris en matière de lutte contre la cybercriminalité, sera réalisé.

3.2.4 Effectifs (ministères publics)

- La plupart des ministères publics cantonaux dispose de procureurs partiellement ou entièrement dédiés à la lutte contre la cybercriminalité. Une minorité de ces procureurs travaille dans une unité dédiée à cette thématique. La création de nouveaux postes varie fortement d'un canton à l'autre. Bien que l'augmentation de poste passée (+22) et prévue (+18) soit relativement importante, elle se concentre sur un nombre limité de cantons.

La majorité des ministères publics cantonaux disposent de procureurs partiellement (14) ou entièrement (6) spécialisés dans le traitement des affaires de cybercriminalité. Six ministères publics n'ont pas de procureurs spécialisés dans ce domaine.

Selon les retours des cantons, ce sont environ 40 procureurs qui traitent entièrement (15) et partiellement (25) des affaires de cybercriminalité. Ces procureurs sont soutenus par une trentaine de collaborateurs. Six ministères publics cantonaux disposent d'une unité dédiée à la lutte contre la cybercriminalité. Ces unités rassemblent la moitié (20) des procureurs partiellement ou entièrement dédiés à la lutte contre la cybercriminalité et la grande majorité du personnel de soutien aux procureurs (25). Au niveau des ministères publics cantonaux, ce sont donc environ 60 personnes qui s'occupent entièrement ou en partie de la lutte contre la cybercriminalité.

Ces dix dernières années, 22 postes supplémentaires ont été créés dans neuf ministères publics cantonaux afin de lutter contre la cybercriminalité. Dans les dix prochaines années, 18 postes supplémentaires devraient être créés au sein de six ministères publics cantonaux.

Et au niveau fédéral? Le MPC dispose d'un domaine spécialisé dans la lutte contre la cybercriminalité. Celui-ci est composé de deux procureurs, trois procureurs assistants ainsi que d'un référent cyber. Ces 6 personnes ont été engagées entre 2016 et 2023.

[68] *L'Ostschweizer Polizeikonkordat* (Ostpol) regroupe les polices cantonales d'Appenzell Rhodes-Extérieures, d'Appenzell Rhodes-Intérieures, de Glaris, des Grisons, de Schaffhouse, de Saint-Gall et de Thurgovie, les polices municipales de Coire et de Saint-Gall ainsi que la Police nationale de la Principauté de Liechtenstein.

3.2.5 Traitement des plaintes

Neuf polices cantonales ont indiqué ne pas être en mesure de traiter toutes les plaintes. En moyenne, ces polices sont en mesure de traiter 70 % des plaintes reçues. Différents critères sont utilisés afin de prioriser le traitement des affaires: le préjudice causé (matériel, financier, réputationnel), le type d'infrastructure touchée (par ex. une infrastructure critique), la typologie du délit (par ex. un délit s'inscrivant dans une série de délits aura plus de chance d'être investigué, pour autant que la série soit identifiée), les chances de succès de l'investigation (qui permettent d'inférer de liens avec l'étranger, de l'existence de traces forensiques, d'une dénonciation rapide du crime) ou encore des mesures d'investigation (par ex. blocage de valeurs). Ces différents critères font que certains délits, tels que les attaques de *ransomwares* (préjudice important) ou la fraude à l'investissement en ligne (préjudice important et séries de délits), sont traités de manière prioritaire.

En matière de traitement de plainte, les pratiques sont très diverses. Ainsi, des spécialistes nous ont indiqué qu'une plainte pouvait être considérée comme traitée lorsqu'elle avait été enregistrée dans la base de données de police. C'est pourquoi de très nombreux cantons ont indiqué traiter 100 % des plaintes, mais cela n'indique pas que pour chacune de ces plaintes, une enquête soit effectivement menée.

En ce qui concerne les raisons qui empêchent de traiter toutes les plaintes, les neuf polices cantonales citent toutes le manque d'enquêteurs, les deux tiers citent le manque d'autres moyens humains (analystes, spécialistes forensiques TI), environ la moitié citent également le manque de moyens techniques ou des plaintes de qualité insuffisante.

3.2.6 Recrutement de personnel

- La plupart des polices cantonales rencontrent des difficultés en matière de recrutement, que ce soit pour des spécialistes TI ou des enquêteurs cyber. De nombreuses raisons expliquent ces difficultés et la plupart des polices mettent en place des mesures pour pallier cela, notamment via la formation continue.

Dix-huit polices cantonales ont indiqué rencontrer des difficultés en ce qui concerne le recrutement de personnel qualifié. Ces difficultés sont particulièrement aiguës pour ce qui est des spécialistes forensiques TI et relativement élevées s'agissant des analystes cyber et des enquêteurs. Ces difficultés s'expliquent par différents facteurs.
Tout d'abord, le nombre de candidats aspirants policiers stagne ou diminue dans certains cantons[69]. Puis, une fois le personnel recruté, il s'agit également de le garder. Le personnel formé représente un investissement important pour le canton formateur. Cet investissement ne peut pas être amorti si le personnel quitte la police cantonale pour un autre corps de police ou encore quitte le métier de policier. Le personnel formé peut également être désabusé car les procédures en matière de cybercriminalité, souvent menées contre inconnu, n'aboutissent que rarement à une condamnation.

Plusieurs solutions sont à la disposition des polices cantonales pour pallier ces problèmes de recrutement. Il s'agit d'abord d'utiliser le personnel existant non spécialisé. Ce personnel peut être formé à la cybercriminalité de manière plus ou moins poussée. Ainsi, la formation Cyber II de l'ISP permettra à un enquêteur d'acquérir les connaissances de base indispensables aux investigations en matière de cybercriminalité. Des formations supplémentaires sont dispensées en Suisse et à l'étranger et permettent une spécialisation poussée des enquêteurs, des analystes criminels ou encore des

[69] Face à la pénurie de main-d'œuvre, les polices romandes peinent à susciter des vocations - rts.ch - Régions

spécialistes forensiques TI**.** Toutefois, il ne s'agit pas uniquement de former des spécialistes, mais aussi de diffuser les connaissances de base de la lutte contre la cybercriminalité auprès de tous les policiers. Ces derniers pourront de la sorte prendre les mesures les plus pertinentes (par ex. demander les bonnes informations lors du recueil d'une plainte) et décharger les spécialistes.

Pour retenir le personnel, les cantons doivent parfois faire preuve de créativité. Les polices cantonales de certains cantons ne peuvent pas rivaliser avec celles d'autres cantons ou avec les entreprises privées en matière de salaire. Il s'agit d'un problème aigu notamment en ce qui concerne les spécialistes en forensique TI, dont les compétences sont très recherchées dans l'industrie privée. Il s'agit alors de mettre en avant d'autres facteurs tels que la mission du service public, les possibilités de suivre des formations continues attrayantes ou encore des conditions de travail adaptées aux attentes.

Malgré toutes ces mesures, il demeure nécessaire de recruter du nouveau personnel pour pallier les départs et répondre à l'augmentation de la cybercriminalité. Le point 3.2.3. le démontre: des postes ont été ouverts ces dix dernières années et un nombre important de postes sera à pourvoir ces dix prochaines années. Il s'agit donc de mettre en œuvre des campagnes de recrutement ciblées. Le recrutement de jeunes peut également être facilité par la création de postes de stagiaires ou par l'accueil de personnes qui suivraient des formations en emploi. De la sorte, ces personnes pourraient découvrir l'univers policier et l'intégrer si les postes le permettent. Il est également possible de recruter des spécialistes qui disposent de compétences techniques rares mais qui ne disposent pas du brevet de policier. Il est alors crucial de leur mettre à disposition la formation nécessaire à leur intégration dans le monde policier. Enfin, il est possible que, pour certaines compétences très spécifiques, le profil recherché ne soit tout simplement pas disponible sur le marché du travail ou qu'il ne soit pas réaliste de former du personnel existant. Il s'agit alors de regarder les possibilités de coopération existantes – par exemple via l'entraide administrative – au niveau régional ou national. Dans certains cas précis, le recours à des prestataires privés représente également une bonne option. Il peut s'agir par exemple de donner des mandats ponctuels à des entreprises de cybersécurité qui disposent de compétences techniques très pointues.

3.3 Moyens techniques

- ❖ La plupart des polices cantonales disposent des moyens techniques nécessaires à une lutte efficace contre la cybercriminalité. Il s'agit toutefois de réévaluer fréquemment l'adéquation des logiciels utilisés et de s'assurer que le personnel compétent est disponible en nombre suffisant.

Les moyens techniques constituent un auxiliaire indispensable aux unités de police judiciaire chargées de lutter contre la cybercriminalité. Une majorité de polices cantonales dispose de logiciels permettant d'analyser les flux de cryptomonnaie (15), d'analyser les réseaux (16) et d'identifier la criminalité sérielle en ligne (15). Une minorité de polices cantonales dispose de moyens facilitant le blocage de valeurs (11) ou permettant d'effectuer une surveillance d'Internet - par exemple des réseaux sociaux ou encore du *darkweb* (9). Certaines polices cantonales indiquent par ailleurs ne pas posséder les outils mais y avoir accès de manière indirecte via des accords avec d'autres corps de police.

Malgré tout, ces outils ne permettent pas de retrouver les auteurs en un clic. Bien que leur utilisation facilite le travail des enquêteurs, ils nécessitent des connaissances spécialisées et génère du travail. De même, l'utilisation de ces outils sur le terrain, par exemple lors d'une perquisition, demande également des ressources spécialisées[70].
En matière de flux de cryptomonnaie, les produits permettent notamment de suivre les flux (mais pas de les stopper) et d'aider les enquêteurs à identifier les auteurs. Néanmoins, ces produits fonctionnent

[70] Cf. aussi rapport GCBF, ch. 7.4.1.

avec des modèles de licences qui sont coûteuses et qui ne couvrent pas toutes les cryptomonnaies. Les outils de monitoring du *darknet* ou par exemple des plates-formes d'échange pair-à-pair sont d'une aide précieuse pour lutter contre la pédocriminalité ou encore le trafic de stupéfiants.

Dans les années à venir, la situation devrait continuer à s'améliorer: un certain nombre de polices cantonales ne disposant pas de certains produits techniques va s'en procurer. Une grande majorité des polices cantonales disposera ainsi des moyens techniques permettant le suivi des flux de cryptomonnaie, d'identifier la criminalité sérielle en ligne ou encore d'effectuer une surveillance d'Internet. Toutefois, de nombreux cantons (10) estiment qu'il manque, à l'heure actuelle, un outil efficace et simple d'usage pour effectuer de la recherche d'information en sources ouvertes (OSINT), que cela soit sur le *clearweb* ou le *darkweb*. Un tel outil représenterait une plus-value pour la très grande majorité des investigations. Il faut noter que les investissements dans de nouveaux moyens techniques, pour être efficaces, doivent également s'accompagner d'investissements en ressources humaines.

3.4 Formation

- ❖ De nombreuses formations entièrement ou partiellement dédiées à la lutte contre la cybercriminalité sont maintenant disponibles en Suisse. De nombreux acteurs (ISP, NEDIK, polices cantonales, universités et hautes école, secteur privé) proposent des formations. Il existe toutefois des thématiques qui ne sont pas ou peu couvertes.

Une grande majorité des polices cantonales a développé des formations internes en matière de lutte contre la cybercriminalité. Ces formations vont des thèmes généraux (introduction à la cybercriminalité) à des thématiques très spécifiques telles que les cryptomonnaies, l'OSINT ou encore le *darknet* et les métavers. Le NEDIK offre également des formations spécialisées qui sont très appréciées des participants. Certains souhaitent que les prestations du NEDIK en matière de formation soient renforcées.

L'ISP a développé un e-learning qui est suivi par l'ensemble des aspirants policiers dans le cadre de l'école de police (le test final a été réussi à 18 796 reprises[71]). Certains participants relèvent que chaque policier devrait suivre à nouveau l'e-learning, notamment lorsque son contenu est mis à jour. Il est également souhaité que la formation de base en matière de cybercriminalité soit plus approfondie et uniformisée dès l'école de police. L'ISP a également développé une formation spécialisée pour enquêteur. Le cours Cyber II est réservé aux membres des polices judiciaires intéressés et l'ISP indique qu'il a été suivi par 841[72] participants depuis sa création.

La grande majorité des participants au sondage estime que les formations de l'ISP en matière cyber sont suffisantes[73]. Il est toutefois souhaité que l'ISP renforce ses formations, principalement en approfondissant les domaines suivants: OSINT, recherches secrètes sur Internet, cryptomonnaies, prévention, analyse des *malwares*, moyens de communication cryptés, analyse de donnée de masse, cyberphénomènes. Plusieurs participants indiquent que le cours Cyber II est suffisant pour un inspecteur de police judiciaire mais insuffisant pour un enquêteur spécialisé en matière de cybercriminalité.

Pour cela, des cours de type *Certificate of Advanced Studies (CAS)* ou *Master of Advanced Studies (MAS)* sont proposés par différentes universités et font offices de prolongement inofficiel de la formation

[71] Mars 2023
[72] Mars 2023
[73] À noter que 27 entités se sont exprimées comme étant soit plutôt d'accord, d'accord ou entièrement d'accord et que 9 entités se sont exprimées comme étant plutôt pas d'accord, pas d'accord ou pas du tout d'accord.

de l'ISP. Les formations suisses sont recensées sur la plate-forme cyberpie.ch[74]. Étant donné les évolutions très rapides en matière de cybercriminalité, il est suggéré que l'ISP s'associe avec les hautes écoles et les universités afin de proposer un programme de formation continue. Celui-ci constituerait la suite du cours Cyber II. Il est également proposé de créer un MAS réservé aux autorités de poursuite pénale et rassemblant plusieurs CAS existants. Ce MAS constituerait le plus haut niveau de spécialisation.

De nombreux participants indiquent suivre des formations dispensées par des universités sises à l'étranger. À noter qu'un nombre important de ces formations concerne des MAS. Cela semble logique, étant donné leur quasi absence en Suisse et du fait que certaines universités étrangères (notamment Dublin) sont précurseurs en la matière. Outre ces formations, il existe également des webinaires ponctuels donnés par des organisations internationales (Interpol, Europol, CEPOL). Un certain nombre d'entreprises mettent également à la disposition de leurs clients des formations spécifiques pour utiliser leurs logiciels.

Seule une minorité de ministères publics a développé des formations internes. Toutefois, il semble que les ministères publics se reposent davantage sur des structures régionales (cours de la Staatsanwaltsakademie[75] ou encore de l'École romande de la magistrature pénale[76]). Les procureurs soulignent qu'il n'y a pas suffisamment de formations en Suisse qui leur sont destinées. Ils souhaitent qu'un cours de type Cyber II, destiné aux procureurs, soit créé. Certains procureurs indiquent également suivre des cours destinés aux policiers.

3.5 Prévention

- Toutes les polices mènent des actions de prévention. Toutefois, les actions de prévention ne sont tout simplement pas assez nombreuses pour faire face à l'augmentation de la cybercriminalité. Elles doivent être renforcées dans toutes les thématiques et cibler l'ensemble de la population. Les polices cantonales sont conscientes de cette situation et la majorité va renforcer ses actions de prévention en matière de lutte contre la cybercriminalité dans les années à venir.

L'ensemble des polices cantonales a organisé des actions de prévention liées à la cybercriminalité ces cinq dernières années. L'ensemble des polices cantonales a également participé à des actions organisées par la PSC. Une minorité de cantons a participé à des actions organisées par d'autres acteurs publics ou privés.

La majorité (43/69) des répondants estime toutefois que les actions de prévention menées à l'heure actuelle sont insuffisantes[77]. Bien qu'une majorité estime que les actions devraient être renforcées dans quasi toutes les thématiques, seule une très faible minorité estime que les mauvaises thématiques sont ciblées. Il s'agit notamment de renforcer les actions en matière de fraude à l'investissement en ligne, d'escroqueries sur les places de marché et de *money mules*[78].

Il est également souligné que les actions de prévention ne sont pas suffisamment nombreuses ou coordonnées et qu'elles ne touchent pas les bons publics. À ce titre, la grande majorité des autorités

[74] Cette plate-forme est le résultat d'un projet mené au sein du groupe de formation dédié à la formation cyber de la CCPCS. À ce jour, elle recense 22 formations.
[75] Home (staatsanwaltsakademie.ch)
[76] École romande de la magistrature pénale (ERMP) - Haute école Arc (he-arc.ch)
[77] L'assertion exacte était: "De manière générale, les actions de prévention menées à l'heure actuelle en matière de cybercriminalité sont suffisantes". Elle a été adressée aux polices cantonales, aux ministères publics ainsi qu'aux tribunaux. Dans le détail: 43 participants ne sont pas d'accord avec cette assertion (5 pas du tout d'accord; 15 pas d'accord; 22 plutôt pas d'accord et 26 participants sont d'accord (1 entièrement d'accord, 5 d'accord, 22 plutôt d'accord).
[78] À l'assertion "Davantage d'actions de prévention doivent être menées dans les domaines suivants", les réponses ont été les suivantes: fraude à l'investissement en ligne (72 %), fausses annonces (63 %), *money mules* (58 %), *romance scams* (55 %), hygiène informatique (55 %), autres cyber-escroqueries (50 %), pédocriminalité en ligne (45 %), discours de haine en ligne (42 %).

interrogées souhaitent que la prévention soit intensifiée auprès de l'ensemble de la population, avec un focus particulier sur les 65 ans et plus. Un répondant note que les personnes n'ayant pas été victimes de cybercriminalité ne se sentent pas concernées par celle-ci. C'est le cas par exemple de nombreuses PME, qui sont conscientes des risques mais ne prennent pas de mesures pour les circonscrire. La cybercriminalité progresse fortement, il faut donc que les efforts de prévention progressent également et qu'ils s'adaptent de manière très rapide aux nouveaux modi operandi.

Il faut toutefois noter qu'en matière de prévention, il est toujours difficile d'estimer l'impact réel de ces campagnes. Ainsi, même si les mesures de prévention sont renforcées, il demeurera très compliqué d'avoir des indicateurs qui démontrent leur impact sur les statistiques policières de la criminalité.

3.6 Mutualisation

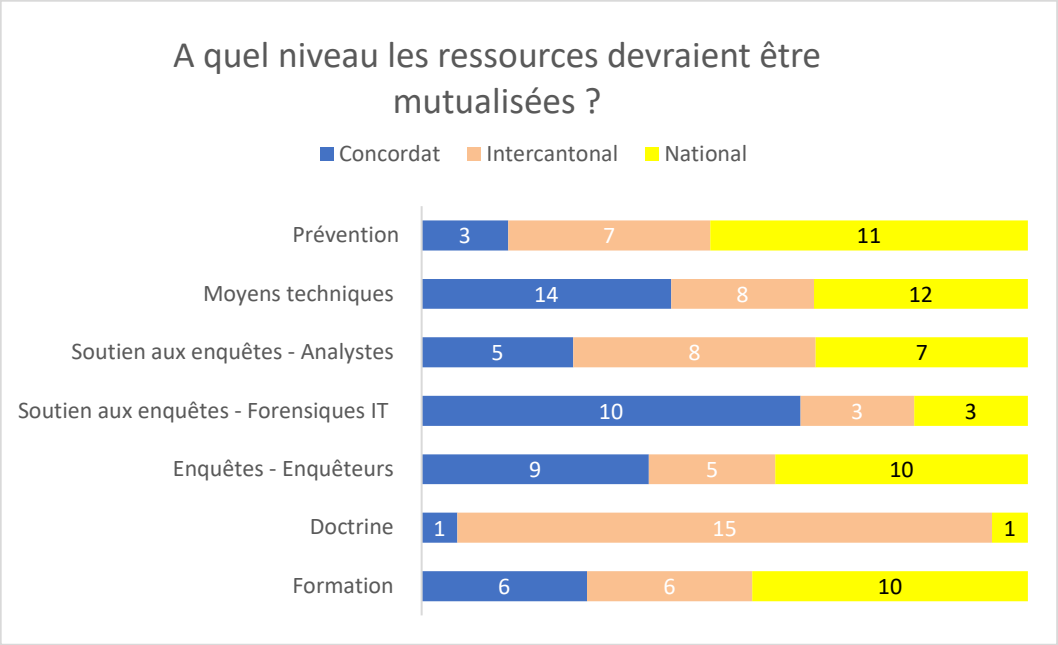
- La quasi-totalité des répondants estiment qu'il est souhaitable que les ressources soient mutualisées afin de lutter contre la cybercriminalité. Il n'existe toutefois pas de consensus sur la manière dont cette mutualisation doit être réalisée. Le travail des entités fournissant des prestations à l'ensemble de la Suisse, telles que le NEDIK, le Cyber-CASE, l'OFCS ou encore fedpol, est généralement très apprécié.

Presque tous les répondants sont d'accord: il est souhaitable de mutualiser les ressources afin de lutter contre la cybercriminalité[79]. La majorité des répondants estime que les ressources devraient être mutualisées dans quasi tous les domaines, à l'exception de la doctrine. Les domaines des moyens techniques, de la formation et de la prévention sont privilégiés pour la mutualisation. En ce qui concerne la formation et la prévention, des structures nationales (ISP, PSC) existent déjà et répondent à ce besoin de mutualisation. La mutualisation des moyens techniques est effectuée via différentes entités (NEDIK, fedpol, TIP).

Selon les participants, les moyens humains en matière d'enquête, de forensique TI et de renseignement criminel devraient également être mutualisés. Pour ce qui est des enquêtes, une mutualisation ne serait toutefois pas évidente car il s'agirait de clarifier au cas par cas les questions de juridiction. Plusieurs participants ont évoqué la possibilité d'un transfert partiel ou complet des compétences de poursuite pénale de la cybercriminalité à la Confédération.

Bien qu'il existe un consensus sur la nécessité de la mutualisation, les positions sont beaucoup moins claires en ce qui concerne les domaines dans lesquelles cette mutualisation devrait intervenir. S'agissant de la forensique TI, la majorité des répondants estime qu'elle devrait intervenir au niveau concordataire; pour ce qui est de la prévention, elle devrait être mutualisée au niveau national tandis que la doctrine devrait être mutualisée au niveau intercantonal.

[79] Quant à l'assertion "Il est souhaitable de mutualiser les ressources afin de lutter contre la cybercriminalité", les réponses ont été les suivantes: tout à fait d'accord: 50 %, d'accord: 27 %, plutôt d'accord: 19 %, plutôt pas d'accord: 2,5 %, pas d'accord: 1,5 %.



Huit polices cantonales ont indiqué mutualiser des ressources humaines en matière de lutte contre la cybercriminalité. En revanche, aucune police cantonale n'a indiqué prévoir de mutualiser des ressources humaines supplémentaires à l'avenir. Il semble que la mutualisation des ressources intervienne en particulier dans le cadre du centre de compétence forensique TI de Zoug, qui offre des prestations aux cantons de Zoug, Schwyz, Nidwald, Obwald et Uri[80]. Le centre de compétence forensique du canton de Saint-Gall[81] offre également ses prestations à tous les cantons du concordat Ostpol[82]. Certains moyens sont également mutualisés au sein du RC3 Romandie (sis à Genève), où un ETP financé par le concordat RBT (Suisse romande, Berne et Tessin) s'occupe du dispositif opérationnel PICSEL. Le RC3 offre également des prestations à tous les cantons romands, notamment en matière de déploiement de logiciels informatiques spéciaux, d'analyse forensique de l'informatique embarquée dans les véhicules ainsi qu'en matière de lutte contre la pédocriminalité. Outre ces trois structures, la mutualisation liée à la cybercriminalité intervient principalement dans les structures intercantonales telles que le NEDIK, la PSC[83] ainsi que l'ISP[84] (voir ci-après). Bien que le canton de Zurich n'appartienne à aucun concordat, il encourage une coopération régionale et soutient les autres cantons sur demande.

En matière de moyens techniques, la mutualisation est bienvenue car elle permet de réduire les coûts des licences pour certains produits informatiques. Une grande majorité des polices cantonales mutualise déjà ou compte mutualiser des moyens techniques, que cela soit au niveau concordataire ou intercantonal. Ainsi, suite à une initiative du NEDIK, un coût unique – et inférieur aux tarifs pratiqués auparavant – pour un logiciel d'analyse de cryptomonnaie a été défini pour toute la Suisse. La mutualisation peut également s'étendre à l'utilisation de logiciels communs tels que PICSEL – maintenant adopté par neuf cantons. La mise à disposition d'outils développés en interne est également une forme de mutualisation. Ici, la police cantonale lucernoise fait figure d'exemple en mettant à disposition plusieurs logiciels.

[80] *IT-Forensik Kompetenzzentrum* (zg.ch)
[81] *Forensik* | sg.ch
[82] Outre Saint-Gall: Appenzell Rhodes-Extérieures, Appenzell Rhodes-Intérieures, Glaris, Grisons, Schaffhouse, Thurgovie ainsi que la Principauté de Liechtenstein.
[83] La PSC est financée via des contributions des cantons et de la Confédération.
[84] L'ISP reçoit des subventions des cantons et de la Confédération.

3.6.1 NEDIK

Près de 5,5 ETP[85] ayant des missions pour l'ensemble de la Suisse sont financés par le NEDIK. Les missions de coordination nationale au niveau stratégique et opérationnel sont assumées par la police cantonale de Zurich (2 ETP). La police cantonale de Berne gère la coordination nationale pour le monitoring des réseaux pair-à-pair dans la lutte contre la pédocriminalité en ligne (2 ETP)[86]. La police cantonale de Saint-Gall s'occupe de la gestion du savoir (0,5 ETP) tandis que la police cantonale de Genève s'occupe de la gestion de PICSEL au niveau national (1 ETP). Des fonds supplémentaires sont disponibles pour différentes prestations telles que l'acquisition de logiciels, la gestion de projet ou encore l'organisation de formations.

La majorité des répondants estime que les prestations du NEDIK sont satisfaisantes[87]. Une grande majorité des répondants estime que le NEDIK apporte une plus-value en matière de réseautage et de transfert du savoir. Une majorité estime également que le NEDIK apporte une plus-value en matière de coordination opérationnelle tandis qu'une minorité estime qu'il apporte une plus-value en matière de coordination stratégique et de formation. Enfin, une petite minorité estime que le NEDIK apporte une plus-value en matière d'unité de doctrine ou de renseignement criminel.

En ce qui concerne le potentiel d'amélioration, celui-ci réside principalement dans la coordination opérationnelle. C'est le seul domaine où une majorité de participants estime que le NEDIK pourrait être amélioré. Dans le détail, les participants aimeraient que le NEDIK coordonne des enquêtes, notamment pour le phénomène des *ransomwares*[88]. Il est également souhaité que le NEDIK aide à la judiciarisation des séries en se coordonnant avec les ministères publics via le Cyber-CASE (voir ci-après). Une coordination avec les procureurs est également souhaitée dans le domaine de la coordination stratégique, certains répondants souhaitant ainsi que le NEDIK et le Cyberboard établissent une politique (cyber)criminelle. Enfin, plusieurs répondants ont mentionné le souhait que le NEDIK négocie les prix d'acquisition de certaines licences ou appareils spécialisés au nom des cantons – ce qui est déjà partiellement le cas.

Ces potentiels d'amélioration sont toutefois limités par différents facteurs. Un participant note ainsi qu'en l'absence de véritables centres de compétence régionaux en matière cyber, le NEDIK ne peut faire office de "réseau des réseaux" et donc atteindre sa plus-value maximale. Les moyens attribués au NEDIK devraient également être réévalués, un participant soulignant que le rôle de chef du NEDIK devrait être une occupation à plein temps.

3.6.2 Cyber-CASE

Bien que le Cyber-CASE soit avant tout un instrument à la disposition des ministères publics, une dizaine de polices cantonales participe à ses séances. Une grande majorité des participants estime que les prestations du Cyber-CASE sont satisfaisantes[89]. Le rôle du Cyber-CASE est particulièrement reconnu en matière de transfert du savoir et de réseautage. De nombreux participants soulignent ainsi la plus-value que représente le fait de pouvoir rencontrer ses homologues, de discuter de cas ou encore d'assister à des présentations sur différents aspects de la cybercriminalité.

Seule une minorité de participants estime que le Cyber-CASE apporte une plus-value dans le domaine de la coordination opérationnelle (fixation de for, discussion sur les cas) tandis qu'une majorité souhaite justement que le Cyber-CASE renforce son action dans ce domaine. Il est notamment souhaité que le

[85] Les moyens financiers sont accordés par la CCDJP à la CCPCS. La CCPCS fait office de mandant du NEDIK.
[86] Pour plus d'informations à ce sujet, voir le rapport du Conseil fédéral en réponse aux postulat Feri-Regazzi.
[87] À l'assertion "Les prestations du NEDIK sont satisfaisantes", les réponses ont été les suivantes (N=26): tout à fait d'accord: 11 %, d'accord: 27 %, plutôt d'accord: 27 %, plutôt pas d'accord: 23 %, pas d'accord: 8 %, pas du tout d'accord: 2 %.
[88] À noter que le NEDIK ne peut pas mener d'enquête, uniquement assurer la coordination en assurant l'échange d'informations.
[89] À l'assertion "Les prestations du Cyber-CASE sont satisfaisantes", les réponses ont été les suivantes (N=37): tout à fait d'accord: 5,5 %, d'accord: 48,5 %, plutôt d'accord: 35,5 %, plutôt pas d'accord: 3 %, pas d'accord: 5,5 %, pas du tout d'accord: 3 %.

Cyber-CASE soit davantage actif dans l'identification précoce de séries liées aux mêmes auteurs afin de faciliter leur reprise par une seule autorité et d'éviter ainsi les enquêtes menées à double. Il est relevé que le Cyber-CASE dispose d'une liste des cas en cours mais que celle-ci n'est que trop rarement tenue à jour par les cantons. Un renforcement du Cyber-CASE au niveau opérationnel est subordonné à la transmission de séries de cas par les ministères publics cantonaux ou par les polices (via le NEDIK par ex.).

Certains participants souhaitent également que le Cyber-CASE renforce son action stratégique, notamment en effectuant un travail de sensibilisation auprès du personnel politique ou en proposant des modifications législatives destinées à faciliter la lutte contre la cybercriminalité.

3.6.3 OFCS

La coopération avec l'OFCS est également importante et s'articule essentiellement autour de deux piliers: la prévention et le savoir-faire technique. En matière de prévention, c'est en particulier celle destinée aux PME et à la population qui est soulignée. Les participants relèvent que le partage des tâches entre l'OFCS et les polices en matière de prévention devrait être amélioré.

La plate-forme d'annonce de l'OFCS et les bulletins hebdomadaires d'information qui en résultent apportent une plus-value également pour les autorités de poursuite pénale. Certains participants souhaitent que l'OFCS dispose de bases légales facilitant sa coopération avec les autorités de poursuite pénale. Une obligation d'annonce de l'OFCS à ces autorités en cas d'attaque sur une infrastructure critique est par exemple évoquée. Au niveau technique, les compétences de l'OFCS sont appréciées. Elles se concentrent notamment via la plate-forme d'information sur les *malwares* (PolMISP) ainsi que sur des soutiens ponctuels dans le cadre d'enquêtes (s'agissant par ex. de l'analyse forensique de *malwares*).

3.6.4 fedpol

La majorité des répondants estime que les prestations de coordination internationale fournies par fedpol sont satisfaisantes[90]. Certains participants estiment que fedpol devrait offrir davantage de services liés à son rôle d'office central, notamment en lien avec l'étranger. Il est également souhaité que l'échange d'informations avec l'étranger soit amélioré, par exemple via l'obtention de bulletins de renseignements criminels d'autres pays ou d'organisations internationales.

La grande majorité des répondants estime également que la Suisse devrait renforcer sa présence auprès des organisations internationales afin d'améliorer la lutte contre la cybercriminalité. Cette prestation pourrait être renforcée par exemple en déployant des attachés de police dans les régions d'origine des auteurs.

3.6.5 Produits de renseignement

Reflétant la complexité de la cybercriminalité et du fédéralisme, plusieurs produits de renseignement criminels sont publiés. Le NEDIK publie ainsi deux produits: un bulletin mensuel qui met en lumière les tendances actuelles et commente certains cas ainsi qu'un bulletin mensuel spécifique dédié à la fraude à l'investissement en ligne (PICSEL OAB). Ce dernier bulletin repose sur l'exploitation nationale – dans le cadre d'un projet pilote – des données enregistrées sur PICSEL.[91]

[90] À l'assertion "Les prestations de coordination internationale fournies par fedpol (office central cyber, bureau de liaison auprès d'Europol, attachés de police) sont satisfaisantes", les réponses ont été les suivantes (N=28): tout à fait d'accord: 10,5 %, d'accord: 35,5 %, plutôt d'accord: 20,5 %, plutôt pas d'accord: 27,5 %, sans réponse: 7 %.

[91] Il ne faut pas confondre PICSEL et PICSEL OAB.
PICSEL vise à analyser tous les phénomènes cybercriminels sériels mais seule une minorité de canton participe au dispositif.
PICSEL OAB est un projet pilote dédié à l'analyse d'un seul phénomène cybercriminel, la fraude à l'investissement en ligne. Une majorité de cantons participe au dispositif. PICSEL OAB se base sur l'infrastructure et la doctrine de PICSEL.

L'ensemble des données recueillies dans PICSEL fait également l'objet d'un bulletin mensuel qui présente les statistiques et les cas saillants. Ce bulletin ne reflète naturellement que les données des neuf cantons participant à PICSEL. L'OFCS publie un bulletin hebdomadaire qui présente et analyse les informations reçues via sa plate-forme de signalement. Les cas intéressants sont également signalés. Enfin, fedpol publie plusieurs rapports chaque année sur des thématiques d'actualité (cryptomonnaie, métavers, intelligence artificielle). Tous les produits évoqués ci-dessus sont disponibles sur une plate-forme gérée par le NEDIK. Cette plate-forme rassemble également les rapports publiés par Europol. Une grande majorité des participants estime que ces produits représentent une plus-value pour leur travail. Le domaine d'amélioration principal identifié est la réduction du nombre de produits. Les participants soulignent également qu'il faudrait que davantage d'informations opérationnelles soient partagées, sur le modèle des bulletins PICSEL, et que ces informations soient diffusées à un rythme plus régulier. La majorité des participants souhaite qu'un tel produit soit édité au niveau intercantonal.

4 Analyse des forces et faiblesses du système actuel

Dans le cadre du sondage, les participants ont été invités à s'exprimer sur les forces et les faiblesses de l'organisation de la Suisse en matière de lutte contre la cybercriminalité. Ces retours ont été synthétisés dans ce chapitre.

4.1 Forces

- Les participants soulignent que la Suisse peut s'appuyer sur de nombreux facteurs de succès en matière de lutte contre la cybercriminalité: des spécialistes bien formés, un réseau formel et informel d'experts qui se connaissent personnellement, de la solidarité entre les cantons ou encore des moyens financiers importants en comparaison internationale sont notamment évoqués.

L'une des forces principales reste le facteur humain. Le personnel est fortement engagé et le niveau de formation générale – y compris en procédure pénale – ainsi que les connaissances linguistiques représentent des atouts non négligeables. La formation en matière de cybercriminalité s'améliore tandis que les possibilités de formation spécialisée se multiplient. Le niveau de spécialisation est également très haut, certaines unités disposant d'experts pointus, que cela soit en matière d'investigation ou de TI. Ces spécialistes forment un réseau informel qui facilite grandement l'échange de connaissances et le retour d'expériences. Du fait de la proximité géographique, les spécialistes se connaissent personnellement, ce qui facilite une collaboration directe et non bureaucratique par-delà les frontières cantonales.

Cette collaboration est une conséquence logique du fédéralisme policier. Bien que celui-ci représente un obstacle pour un domaine aussi transnational que la cybercriminalité, il a également des avantages. Ainsi, la diversité des approches entre cantons est enrichissante, elle permet de confronter les idées, voire d'amener de nouvelles approches dans les enquêtes. Le fédéralisme ne signifie pas "chacun pour soi": certains cantons relèvent ainsi que les "grands" cantons soutiennent volontiers les "petits". Le canton de Zurich est ici cité en exemple, notamment de par sa disponibilité à reprendre des procédures initiées dans d'autres cantons. Ce soutien est toutefois naturellement conditionné à la disponibilité de ressources, ce qui est de moins en moins le cas. Le fédéralisme permet également une proximité de

terrain précieuse, chaque police cantonale – voir municipale – disposant d'un ancrage territorial fort. Cela permet également d'assurer une réaction rapide suite à une dénonciation. Le fédéralisme induit également une capacité d'adaptation élevée, qui se manifeste tant au niveau opérationnel que dans la création de structures de coordination intercantonales.

Ces structures viennent pallier les limites du fédéralisme. Ainsi, le NEDIK ou le Cyber-CASE poursuivent un même objectif: faciliter la lutte contre la cybercriminalité en encourageant la collaboration par-delà les frontières cantonales. Cette collaboration prend de nombreuses formes, que cela soit des réunions opérationnelles, le transfert d'informations sur de nouveaux phénomènes, une unité de doctrine, ou encore la gestion du savoir. D'autres centres de compétence régionaux (RC3, centres de compétence forensique de Zoug ou de Saint-Gall) permettent également de mutualiser les ressources et de combattre des phénomènes criminels en ayant une vue régionale.

Le haut niveau économique de la Suisse est également un avantage. D'une part, il permet de doter les autorités de poursuite pénale de moyens financiers adéquats (en comparaison internationale), ce qui permet un haut niveau de formation et l'acquisition de moyens techniques de pointe. D'autre part, les autorités de poursuite pénale peuvent s'appuyer sur un maillage étroit de hautes écoles et d'universités et d'autres partenaires (par ex. fondation SWITCH). Cela encourage les collaborations avec des acteurs académiques, dont l'outil PICSEL est un résultat.

Au niveau international, la Suisse dispose d'un bon réseau, notamment du fait de sa présence auprès d'Europol et d'Interpol ainsi que des relations bilatérales étroites avec un certain nombre de pays-clefs en matière de lutte contre la cybercriminalité. La participation de la Suisse à la Convention Cyber de Budapest représente également un avantage, dans la mesure où les autorités de poursuite pénale suisses bénéficient de ses instruments (demandes d'information, de préservation et de transmission des données). La Suisse dispose également de bases légales obligeant les prestataires de services à sauvegarder les données pendant six mois, ce qui n'est pas le cas dans de nombreux pays (durée plus courte ou aucune obligation).

4.2 Meilleures pratiques

Le renseignement criminel, notamment via le dispositif PICSEL, apporte une plus-value importante pour les cantons participants. Le projet pilote PICSEL OAB est également cité en exemple: il a permis d'apporter une vue de la situation à l'échelle du pays sur un phénomène précis et de détecter des séries, coordonner des investigations et chiffrer les dégâts causés. Le NEDIK met également à disposition une vue d'ensemble des cas de *ransomwares*, ce qui permet de savoir rapidement quel canton mène une procédure concernant quelles attaques et – le cas échéant – de rassembler des procédures.

La coopération nationale est indispensable. À ce titre, les grands cantons soutiennent parfois les autres cantons. La coopération est également institutionnalisée. Les séances opérationnelles du NEDIK ou encore de l'OSINT Community sont citées en exemple. La coopération avec l'OFCS apporte une plus-value qui pourrait être encore approfondie. La coopération avec les prestataires privés (banques, plates-formes de vente en ligne) pour lutter contre les escroqueries en ligne est positive. La contribution de fedpol en matière de coopération internationale est soulignée, notamment via sa présence au sein du JCAT ou via les prestations de l'office central cyber, par exemple en matière de requêtes auprès des providers.

S'agissant de la formation, c'est le système des trois niveaux qui est mentionné en exemple. Le policier doit recevoir une formation qui lui donne une connaissance générale sur les phénomènes, afin de pouvoir recueillir les informations les plus pertinentes lors du dépôt de plainte. L'enquêteur doit connaître les tactiques d'enquête les plus appropriées afin d'identifier les auteurs, en particulier lorsqu'il s'agit de

criminalité numérique (cours Cyber II). L'enquêteur spécialisé en cybercriminalité doit en plus disposer de compétences techniques qui lui permettent de prendre les meilleures mesures dans les cas les plus complexes de cybercriminalité (CAS / MAS). Il faut que la formation des autorités de poursuite pénale soit régulièrement adaptée afin de refléter les évolutions technologiques rapides. Des échanges à l'interne des corps, entres spécialistes et avec les procureurs, permettent de garantir la transmission des meilleures pratiques.

En matière de prévention, la collaboration de la PSC avec les cantons est jugée positivement. Les efforts de prévention ciblée, notamment auprès d'adolescents et de personnes âgées, sont porteurs. Pour ce dernier groupe, il s'agit de privilégier une communication simple basée sur des faits réels à des heures de grande écoute, par exemple avant le téléjournal. En ce qui concerne les jeunes, la communication doit s'axer autour des réseaux sociaux, la police cantonale vaudoise faisant ici figure d'exemple via le projet "e-cop", soit un policier postant régulièrement du contenu sur tik-tok[92].

Afin de lutter efficacement contre la cybercriminalité, la réactivité est primordiale. Il s'agit notamment de sécuriser rapidement les données en Suisse et à l'international. L'obtention de ces dernières peut ensuite être réalisée parfois simplement via la CCC. Le suivi des flux financiers – comme dans d'autres domaines de criminalité – est très important. Il s'agit de porter un coup aux auteurs en les privant de l'infrastructure informatique qui leur permet d'agir. Pour cela, c'est la coopération internationale, par exemple via des équipes d'enquêtes communes (JIT), qui est indispensable.

4.3 Faiblesses

- De nombreuses faiblesses existent toutefois: les participants ont notamment mentionné les moyens humains très insuffisants, des bases légales (échange automatique d'informations de police, entraide internationale en matière pénale) pas assez adaptées ou encore un morcellement des ressources dû au fédéralisme et une prévention encore insuffisante.

De nombreux participants ont relevé que les ressources humaines sont à l'heure actuelle très insuffisantes. Cela concerne à la fois la police et les ministères publics. Il est ainsi relevé que les ressources à disposition ne permettent tout simplement pas d'enquêter de manière approfondie sur toutes les plaintes reçues. Cela affecte tous les cantons et en particulier les petits cantons qui n'ont pas suffisamment de ressources pour en dédier à la lutte contre la cybercriminalité. Les efforts de prévention sont également touchés par le manque de ressources humaines. Il est relevé que le manque de ressources est aggravé par l'augmentation des dénonciations. Il n'est plus possible de compenser ce manque uniquement via l'optimisation des processus. Une simple réallocation des ressources existantes n'est pas non plus souhaitée, car elle aurait des répercussions sur les autres tâches de police. Un renforcement, via de nouvelles créations de poste, est donc souhaité.

En matière de bases légales, c'est principalement la lenteur et la complexité du régime d'entraide internationale en matière pénale qui est pointé du doigt par de nombreux participants[93]. Cette lenteur est particulièrement problématique dans la mesure où elle permet aux auteurs d'infractions de masquer leurs traces. Au niveau suisse, l'absence de bases légales permettant l'échange automatique d'informations de police est également très problématique[94]. Il est souhaité que des efforts conséquents soient mis en œuvre pour lever rapidement les blocages liés aux bases légales cantonales. À cela s'ajoutent des règles de for considérées comme désuètes par rapport à la cybercriminalité. La

[92] François, le policier vaudois d'Internet qui doit parler aux jeunes - rts.ch - Vaud
[93] Un participant résume ainsi laconiquement la problématique: "Les demandes d'entraide judiciaire prennent beaucoup de temps et devraient être simplifiées au niveau international. Les auteurs d'infractions atteignent des millions de personnes en quelques secondes, alors que les autorités de poursuite pénale n'arrivent même pas à entrer en contact les unes avec les autres pendant des mois. La plupart du temps, les malfaiteurs se trouvent à l'étranger, hors d'atteinte des autorités suisses. Les réponses devraient arriver en temps utile".
[94] La problématique est ainsi évoquée par un spécialiste: "Je reçois davantage d'informations des autres pays de l'espace Schengen que des polices cantonales des cantons voisins".

problématique est aggravée par des compétences de poursuite pénale fragmentées. D'autres aspects, tels que la lourdeur et le coût de certaines procédures de surveillance des communications électroniques (live ou rétroactive), sont également soulignés.

Déjà évoqué dans les bases légales, le fédéralisme est également perçu comme une faiblesse de la Suisse. Celui-ci complique la coordination et la mutualisation des ressources. Il induit un morcellement des ressources, en particulier dans les petits cantons. Les petits cantons n'ont pas les ressources nécessaires pour lutter efficacement contre la cybercriminalité mais n'ont pas non plus un volume de cas suffisant pour mettre en place des unités dédiées. Cela induit qu'ils ne peuvent généralement pas traiter efficacement les cas plus complexes de cybercrime. En l'absence de centre régionaux de compétences, ils doivent s'en remettre à la solidarité des grands cantons.

Ce morcellement a également un impact sur les outils techniques: à défaut de développements ou d'achats groupés, ceux-ci sont réalisés canton par canton. Parfois, c'est le "chacun pour soi" qui subsiste, accompagné d'une réticence à reprendre des cas qui concernent plusieurs cantons. Lorsque les cas ont de fortes ramifications internationales, il est souhaité que la Confédération reprenne le lead. En l'absence d'un système d'enquête national ou d'un système national de renseignement criminel, le risque est grand que les mêmes groupes d'auteurs fassent l'objet de plusieurs procédures non coordonnées. Plusieurs participants relèvent que la multiplication des instances (OFCS, NEDIK, Cyber-CASE, ministères publics, polices cantonales, fedpol, SRC Cyber) partiellement impliquées dans la lutte contre la cybercriminalité complexifie la situation. En termes de coopération internationale, le statut de la Suisse d'État associé à Europol est également un facteur limitant la coopération.

En matière d'enquête, il est relevé que les procédures et les auteurs sis à l'étranger finissent rarement au tribunal. Cela induit un sentiment de travail de répression dans le vide, où même si les auteurs sont identifiés, leur extradition est rendue quasi impossible de par leur présence dans des juridictions pas ou peu coopératives. Outre ces limites, les participants soulignent également le défi posé par la masse de plus en plus importante de données saisies à analyser. Parfois, par exemple pour les recherches sur le *darknet*, c'est le problème inverse qui se pose, respectivement de retrouver des traces forensiques et de les rattacher à un auteur.

De manière générale, un manque de prévention est déploré. Certains répondants relèvent l'absence de hotline pour informer les particuliers. Des campagnes de prévention plus innovantes, par exemple des campagnes de phishing à des fins de sensibilisation, sont recommandées. Une implication plus grande des acteurs privés – dont les services sont souvent détournés – est souhaitée. Un recours plus massif à la prévention technique est attendu.

5 Nécessité d'agir

En se basant sur les défis identifiés au chapitre 2.3 ainsi que sur les résultats du sondage, cinq domaines où il y a nécessité d'agir sont identifiés. Ces domaines correspondent à des problématiques qui ont déjà été soulignées lors de l'élaboration de la CSN, à laquelle les autorités de poursuite pénale cantonales ont été étroitement associées.

Permettre le renseignement criminel cyber via l'échange intercantonal automatique d'informations de police

En l'absence d'échange intercantonal automatique d'informations de police, il est très compliqué pour les polices de savoir quel corps mènent quelles enquêtes contre quels auteurs. Pour ainsi dire, la police ne sait pas ce que sait la police. Cela entraîne une lourde charge de travail inutile (vérification au cas par cas), fait courir le risque que des enquêtes soient menées à double et empêche le développement

d'un renseignement criminel national. Seule une minorité de cantons dispose des bases légales permettant l'échange intercantonal automatique d'informations de police.

- **Mesure en cours:** la mise en œuvre de la motion 18.3592 par les cantons et la Confédération au moyen de la plate-forme de recherche nationale (POLAP) progresse. L'échange d'informations entre les polices, en Suisse et à l'étranger, s'en trouve grandement simplifié. Toutefois, les cantons ne disposent le plus souvent pas des bases légales nécessaires à l'échange d'informations de police en dehors d'une procédure au sens du CPP. Cette lacune devrait être comblée par la nouvelle "Convention intercantonale sur l'échange de données à des fins d'exploitation de plates-formes de recherche et de systèmes de bases de données communs". Ce concordat, qui fixe immédiatement des règles de droit, se trouve actuellement dans la phase de consultation menée par la CCDJP auprès des cantons et de la Confédération. Cette dernière soutient la voie du concordat engagée par la CCDJP et la CCPCS. Si le concordat ne devait pas aboutir, il faudrait que la Constitution fédérale soit modifiée et que l'échange de données de police au niveau national soit réglé par la Confédération pour que la motion puisse être mise en œuvre intégralement. Une motion de la CPS-N allant dans ce sens est actuellement traitée au Parlement (motion 23.4311 "Création d'une base constitutionnelle visant à réglementer l'échange de données de police au niveau national").

Le renseignement criminel permet de faire des liens entre les auteurs, de détecter des tendances et de prendre des mesures préventives. Il représente une plus-value importante pour la lutte contre la cybercriminalité, d'autant plus dans un pays fédéral. Seule une minorité de cantons participe au dispositif PICSEL.

- **Mesures en cours:** à court terme, il faut que tous les cantons disposant d'une base légale examinent l'opportunité de participer à PICSEL. En parallèle, il faut que le projet TIP "PICSEL CH" soit mené à bien. Celui-ci a pour objectif de déployer PICSEL ou une solution similaire à l'échelle de la Suisse. La réalisation de ce projet est également liée à l'adaptation des bases légales permettant aux cantons d'échanger automatiquement des informations de police entre eux. La mesure M13 de la CSN a également pour objectif de régler cette problématique[95].

Adapter les bases légales afin de faciliter la lutte contre la cybercriminalité

Que cela soit pour obtenir des moyens de preuve ou pour traduire les auteurs d'infractions en justice, les autorités de poursuite pénale se heurtent trop souvent aux limites de l'entraide judiciaire internationale en matière pénale La situation actuelle n'est pas satisfaisante et implique de lourdes inefficiences (ralentissement des enquêtes, impunité des auteurs). La Suisse doit intensifier ses efforts pour intégrer les mécanismes existants qui visent à adapter les bases juridiques pertinentes aux développements technologiques. Il s'agit principalement du deuxième protocole additionnel à la Convention de Budapest, du paquet législatif e-evidence de l'Union européenne ou encore du *CLOUD Act* des États-Unis. L'OFJ a posé les bases de la discussion en 2021 puis en 2023[96]. Ces travaux sont en cours de concrétisation afin qu'une décision de principe soit prise. En complément à ces mesures, il s'agirait également d'étudier la conclusion d'accords de police bilatéraux avec les pays où résident les auteurs les plus prolifiques. Une telle mesure serait subordonnée au développement d'un renseignement cybercriminel national. C'est sur la base de celui-ci que les pays prioritaires seraient déterminés.

- **Mesures en cours:** les enjeux de l'entraide judiciaire internationale en matière pénale sont évoqués dans trois mesures de la CSN:

[95] Extrait de la Mesure 13: "Tous les cantons n'y participent toutefois pas encore. Cette situation s'explique par l'absence d'une base légale commune et uniforme qui permettrait à PICSEL d'œuvrer à l'échelle de toute la Suisse. Il convient de déterminer comment créer la base légale requise pour mettre en place une plate-forme garantissant l'échange d'informations".
[96] (Office fédéral de la justice, 2023)

> M12 "Coordonner la collaboration avec les acteurs nationaux et internationaux, principalement dans les domaines de la conservation des preuves ainsi que de l'entraide judiciaire";
> M16 "Assurer une participation active de la Suisse au développement et à la mise en œuvre de la Convention sur la cybercriminalité (Convention de Budapest) du Conseil de l'Europe";
> M17 "S'efforcer de conclure des accords bilatéraux instituant une aide réciproque dans la lutte contre la cybercriminalité".

Outre l'entraide judiciaire internationale en matière pénale, de nombreuses autres bases légales devraient être vérifiées afin de s'assurer qu'elles sont adéquates pour lutter contre la cybercriminalité[97]. Il s'agit notamment d'éclaircir les règles de for – dont la détermination fait souvent perdre du temps dès le début des enquêtes. Explorer des mécanismes innovants tels que des obligations en matière de cybersécurité, la possibilité de faire des perquisitions en ligne, se pencher sur la régulation des cryptoactifs, faciliter la coopération publique-privée à des fins de prévention technique.

Renforcer la coordination en matière de lutte contre la cybercriminalité
De manière générale, il ne faut pas créer de nouveaux organes de coordination mais renforcer ceux qui existent déjà. La coordination opérationnelle en matière de lutte contre la cybercriminalité est assurée par le NEDIK. Pour faire face à l'augmentation de la cybercriminalité, il s'agit d'étudier les mesures pour renforcer le NEDIK, de vérifier que l'accord du NEDIK et le catalogue de prestations correspondent aux besoins et enfin de vérifier si les ressources humaines à disposition sont suffisantes.

Le renforcement de la coopération au niveau national et régional, par exemple via les concordats de police, devrait être étudié. Cela peut consister en la concrétisation de centres de compétence cyber régionaux ou encore dans le fait que certains cantons se spécialisent dans certains domaines au profit des autres membres des concordats et afin d'éviter les doublons. Il s'agit également de vérifier dans quelle mesure des équipes d'enquête communes peuvent être mises en place. Afin d'harmoniser les pratiques au niveau national, il faut examiner dans quelle mesure il serait possible d'établir une stratégie de lutte contre la cybercriminalité. Au niveau de la Confédération, il s'agit de vérifier dans quelle mesure les prestations de coordination internationale peuvent être renforcées, par exemple en matière d'échange international d'informations de police ou de diffusion des rapports de renseignement. Il s'agirait par exemple de renforcer le bureau de liaison suisse auprès d'Europol et d'Eurojust.

En matière de prévention, il s'agit notamment d'intensifier l'organisation de campagnes innovantes au niveau national et d'adapter le calibrage des produits de prévention selon le public cible[98]. Il s'agit également de renforcer l'engagement, le soutien et la participation des autorités cantonales de poursuite pénale aux campagnes nationales de prévention. Pour ce faire, il faudrait également renforcer le lien entre le NEDIK et la PSC. Il faut examiner dans quelle mesure le déploiement d'une plate-forme nationale uniquement dédiée à la prévention de la cybercriminalité serait pertinent (par ex.: cybercrimepolice.ch). Il faut également étudier les moyens de renforcer l'implication des partenaires privés dans les mesures de prévention. Il s'agit enfin de systématiser la prise de mesures de prévention techniques. La sensibilisation de la population aux cyberrisques est prévue par la CSN[99].

- **Mesure en cours:** le renforcement de la collaboration est également prévu par la M12 de la CSN: "Renforcer la collaboration déjà en place: normaliser les processus ainsi que les interfaces et encourager les échanges d'expériences […]. Regrouper les compétences professionnelles (par ex. en forensique informatique) et les achats se rapportant à la sécurité".

[97] Il s'agit d'ailleurs d'un des points relevés dans la CSN. **M12** « À cet effet, il convient notamment d'examiner quelles modifications il serait nécessaire d'apporter aux bases légales […] Les règles locales régissant les compétences en matière de poursuites pénales entravent l'action de la justice pénale contre la cybercriminalité. »
[98] De nombreuses campagnes répondent déjà à ce besoin: SUPER, Campagne card security phishing, Pharming and co.
[99] **M2** "Il convient de vérifier en permanence les besoins de sensibilisation et de prévention dans les différents domaines. Les incidents actuels et l'évolution de l'état de la menace serviront ici de point de départ, tout comme les estimations des autorités, des entreprises et des associations économiques sur le besoin de sensibilisation dans leurs secteurs respectifs.[…] Les acteurs s'occupant de sensibilisation sont connus et leurs échanges font l'objet d'encouragements ciblés. […] Il convient de passer en revue les efforts consentis et les effets obtenus afin de déterminer le succès des mesures de sensibilisation adoptées et de les optimiser".

Adapter les moyens à l'augmentation de la cybercriminalité
Bien que le sondage démontre que la plupart des cantons ont consenti des efforts pour dédier ou recruter du personnel pour lutter contre la cybercriminalité, de très nombreux répondants estiment que les ressources dédiées sont très insuffisantes. Il conviendrait donc en premier lieu d'augmenter les effectifs dans les ministères publics et les polices afin de pouvoir faire face à l'augmentation constante des cas et à leur complexification croissante.
En outre, de nombreux corps de polices utilisent les mêmes moyens techniques mais se les procurent de manière individuelle. Il en résulte une certaine inefficience: prix des licences élevé, formations dispersées. Il s'agit donc de renforcer les efforts visant à centraliser ou à mutualiser l'acquisition de moyens techniques. L'acquisition de nouveaux moyens techniques doit continuer à faire l'objet de réflexions communes. Il s'agit également de renforcer les partenariats pour obtenir de tels moyens techniques auprès d'autres pays ou centres de compétence. Des efforts en ce sens sont déjà en cours via le NEDIK (analyse des cryptomonnaies) et fedpol/TIP (outils de forensique IT). Par ailleurs, la CSN traite également cette thématique[100].

- **Proposition de mesure:** les ressources humaines et techniques affectées à la lutte contre la cybercriminalité relèvent entièrement de la compétence de chaque canton. Bien que des données quantitatives aient été recueillies dans le cadre du sondage, il est conseillé à chaque canton de réaliser une auto-évaluation. L'objectif de cette auto-évaluation serait de déterminer si les moyens actuels suffisent à lutter efficacement contre la cybercriminalité.
- Le postulat 23.4349 "Examen des ressources de fedpol" de la Commission des finances du Conseil national[101] demande de vérifier si les ressources à disposition de fedpol, également en matière de cybercriminalité, sont suffisantes. Le postulat a été adopté par le Conseil national le 28 février 2024.

La formation des autorités de poursuite pénale, que cela soit des policiers, des procureurs et des juges, est importante. Dans un domaine aussi dynamique que la cybercriminalité, il faut s'assurer que les formations sont à jour. Dans l'idéal, un niveau de certification de type "Master of Advanced Studies – MAS" suisse, regroupant des formations existantes, est créé. Il s'agit de s'assurer que les procureurs et les juges aient également accès à des formations ad hoc.

- **Mesure en cours:** la mesure M14 "Formation des autorités de poursuite pénale" de la CSN couvre cette thématique.

6 Conclusions et prochaines étapes

La cybercriminalité augmente constamment, à la fois en termes de quantité de délits et de gravité des dommages causés. La très grande majorité des cantons s'est adaptée pour faire face à cette augmentation de la cybercriminalité. Ces adaptations portent sur la création d'unités dédiées à la lutte contre la cybercriminalité au sein des polices cantonales et sur la création de postes de travail d'enquêteurs, de spécialistes forensiques TI ainsi que d'analystes. Ces créations de postes devraient continuer ces dix prochaines années. Les créations de postes diffèrent fortement d'un canton à l'autre. La majorité des ministères publics cantonaux et le MPC disposent de procureurs spécialisés dans la lutte contre la cybercriminalité.

[100] M12 "Regrouper les compétences professionnelles (par ex. en forensique informatique) et les achats se rapportant à la sécurité".
[101] 23.4349 | Examen des ressources de fedpol | Objet | Le Parlement suisse (parlament.ch)

De nombreux participants au sondage estiment toutefois que les effectifs actuellement dédiés à la lutte contre la cybercriminalité sont très insuffisants et ne permettent pas de traiter les plaintes reçues de manière approfondie. Les participants ont aussi souligné qu'ils souhaitaient disposer d'effectifs supplémentaires, et non pas une réallocation des ressources existantes. Le Conseil fédéral recommande donc à chaque canton de procéder à une auto-évaluation afin de vérifier l'adéquation des moyens investis avec la situation en matière de cybercriminalité.

La collaboration entre cantons – encore plus nécessaire en matière de lutte contre la cybercriminalité – est garantie par le développement d'entités intercantonales comme le NEDIK ou le Cyber-CASE. La problématique est également intégrée dans les activités d'autres entités existantes comme la PSC ou l'ISP. Les prestations de ces différents organes sont très appréciées des spécialistes. De nombreuses autres formes de coopération existent, telles que le centre de compétence cyber en Suisse romande, ou les centres de compétence forensique de Zoug et du concordat de police Ostpol. Ces formes de coopération institutionnalisée sont complétées par des coopérations informelles au cas par cas, par exemple lorsque des cantons mieux dotés reprennent des procédures initiées dans d'autres cantons ou les soutiennent via d'autres prestations.

Se référant également aux suggestions du postulat 22.3017 déposé par la CPS-N, le Conseil fédéral constate que le développement de capacités par les cantons ainsi que l'institutionnalisation d'une coordination intercantonale en matière de lutte contre la cybercriminalité plaide en défaveur d'une reprise complète des compétences de poursuite pénale par la Confédération. Cette mesure est évoquée par une minorité des participants au sondage. Une mise en œuvre de cette mesure reviendrait à remettre en cause la souveraineté cantonale en matière de sécurité d'une part, de même que les efforts organisationnels et les investissements consentis par les cantons pour faire face à cette forme de criminalité d'autre part. Elle serait en outre contraire aux règles posées par le CPP en la matière. Une telle mesure engendrerait également des besoins en personnel très importants au niveau de la Confédération. C'est pour ces mêmes raisons que la création d'un centre de compétence dédié à l'analyse des cryptomonnaies au sein de la Confédération pour les cantons n'est pas pertinente. Les autorités de poursuite pénale cantonales sont maintenant régulièrement confrontées aux cryptomonnaies dans le cadre de leurs procédures pénales. Elles ont déjà commencé à s'équiper et à former leur personnel. Grâce au NEDIK, un prix suisse unique pour un outil d'analyse des cryptomonnaies a été fixé. La Confédération estime qu'il s'agit de l'exemple à suivre.

Deux entraves importantes à une amélioration de la lutte contre la cybercriminalité doivent être mentionnées: l'absence de bases légales permettant l'échange automatique d'informations de police entre les cantons et avec la Confédération d'une part et le régime de l'entraide judiciaire internationale, relativement lent et non adapté aux preuves électroniques, d'autre part.

En l'absence d'échange automatique d'informations de police, il est très compliqué de faire des liens entre des procédures menées dans différents cantons sur les mêmes auteurs. Cela induit un gaspillage de ressources et amenuise les chances de réussite des enquêtes. Cela empêche également le développement du renseignement criminel sur la cybercriminalité au niveau suisse. Or, celui-ci est primordial lorsqu'il s'agit de développer des mesures de prévention techniques ou de sensibilisation de la population, voire de développer des stratégies cohérentes en matière de lutte contre la cybercriminalité. En son absence, il est également très compliqué de consolider des procédures concernant les mêmes auteurs, que cela soit au niveau cantonal ou fédéral. Cette faille est en train d'être résolue via la mise en œuvre de la motion 18.3592 Eichenberger. En parallèle, TIP Suisse mène un projet pour déployer une solution similaire à PICSEL au niveau suisse.

En ce qui concerne l'entraide judiciaire internationale, elle peut constituer un défi pour les enquêtes. Ses limites (lenteur, droits de recours étendus, complexité administrative et problème que l'entraide judiciaire internationale n'est pas adaptée aux preuves électroniques), notamment en dehors du cadre

de la Convention de Budapest sur la cybercriminalité ou Convention du Conseil de l'Europe sur la cybercriminalité, peuvent être un avantage pour les cybercriminels et augmentent leurs chances d'échapper à la justice. Même lorsque les enquêtes sont menées à bien, il s'avère que de nombreux auteurs s'abritent dans des pays avec lesquels l'entraide judiciaire est très compliquée ou ne fonctionne pas. En plus de la Convention de Budapest sur la cybercriminalité et son deuxième protocole additionnel, qui visent à améliorer la lutte contre la cybercriminalité, certains pays de l'UE et les États-Unis ont créé différents actes législatifs et bases juridiques pour faire face aux progrès technologiques dans le domaine de l'entraide judiciaire[102]. L'administration fédérale observe attentivement les évolutions internationales en la matière[103] et a posé des bases de discussion, par exemple concernant le projet e-evidence de l'Union européenne[104]. Ces travaux sont en cours de concrétisation afin qu'une décision de principe puisse être prise.

Selon les retours des autorités cantonales consultées, d'autres domaines doivent également faire l'objet d'améliorations. Les mécanismes de coopération existants (NEDIK, Cyber-CASE) doivent être renforcés et les efforts de prévention augmentés et adaptés pour toucher l'ensemble de la population et des entreprises du pays. Lors de l'acquisition de moyens techniques, il s'agit de privilégier une négociation pour l'ensemble des corps de police plutôt qu'au cas par cas. Le cadre légal, par exemple en matière de fixation de for ou d'obligation des prestataires privés (prévention via leur utilisateur, dénonciation des abus, prévention technique des abus), doit être analysé et si nécessaire faire l'objet de propositions de modification. La coopération internationale doit être intensifiée.

La plupart des recommandations présentées dans ce rapport sont déjà évoquées dans le cadre de la CSN. En effet, les autorités de poursuite pénale avaient été étroitement impliquées lors de son élaboration. Par conséquent, le Conseil fédéral estime que les mécanismes d'implémentation prévus par la CSN – respectivement son comité de pilotage – sont pertinents pour assurer l'amélioration des conditions de lutte contre la cybercriminalité.

[102] (Office fédéral de la justice, 2023), p. 3. Les États-Unis ont adopté le *Clarifying Lawful Overseas Use of Data Act (Cloud Act)* en novembre 2018, qui a pour but de permettre aux autorités de poursuite pénale d'accéder plus facilement aux données stockées à l'étranger. L'UE a adopté le paquet législatif *e-evidence* pour créer un cadre législatif cohérent dans le droit de l'UE afin de régler l'accès aux preuves électroniques et d'accélérer leur obtention.
[103] *US Cloud Act, e-evidence* de l'UE, 2e protocole additionnel à la Convention de Budapest, Convention de l'ONU sur la cybercriminalité.
[104] (Office fédéral de la justice, 2023)

Glossaire

ACPJS	Association des chefs de police judiciaire de Suisse
CAS	Certificate of Advanced Studies
CCC	Convention sur la Cybercriminalité
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
CCPCS	Conférence des commandantes et des commandants des polices cantonales de Suisse
CLCPC	Conférence latine des commandantes et des commandants des polices cantonales
CMP	Conférence suisse des ministères publics
CNFVH	Collection nationale de fichiers et de valeurs de hash
CP	Code pénal suisse
CPJ	Commission de police judiciaire
CPP	Code de procédure pénale suisse
CPS-N	Commission de la politique de sécurité du Conseil national
CSN	Cyberstratégie nationale
DFJP	Département fédéral de justice et police
EC3	European Cybercime Centre
FBI	Federal Bureau of Investigation
fedpol	Office fédéral de la police
FIU	Financial Intelligence Unit
FSFP	Fédération suisse des fonctionnaires de police
IOT	Internet of Things
ISP	Institut suisse de police
JCAT	Joint Cybercrime Action Taskforce
LOC	Loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres États
MAS	Master of Advanced Studies
MPC	Ministère public de la Confédération
MROS	Money Reporting Office Switzerland
NCMEC	National Center for Missing and Exploited Children
NEDIK	Réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique
OFCS	Office fédéral de la cybersécurité
OFDF	Office fédéral de la douane et de la sécurité des frontières
OFJ	Office fédéral de la justice
OFS	Office fédéral de la statistique
PICSEL	Plate-forme d'information sur la criminalité sérielle en ligne
PSC	Prévention suisse de la criminalité
RC3	Centre de compétence cyber régional
RNS	Réseau national de sécurité
SOCTA	Serious and Organised Crime Threat Assessment
SVR-ASM	Association suisse des magistrats de l'ordre judiciaire
TIC	Technologies de l'information et de la communication
TIP	Technique et informatique policières Suisse
TOR	The Onion Router
UE	Union européenne

VPN	Réseau privé virtuel

Bibliographie

Conseil fédéral. (2023). *Cyberstratégie nationale (CSN).*

Eidgenössiche Finanzmarktaufsicht FINMA. (2022). *Kryptobasierte Vermögenswerte.*

European Union Agency for Law Enforcement Cooperation. (2021). *EUROPOL SPOTLIGHT - CRYPTOCURRENCIES: TRACING THE EVOLUTION OF CRIMINAL FINANCE.*

European Union Agency for Law Enforcement Cooperation. (2021). *Internet Organised Crime Threat Assessment.*

European Union Agency for Law Enforcement Cooperation. (2022). *4 TH ANNUAL SIRIUS EU DIGITAL EVIDENCE SITUATION REPORT.*

European Union Agency for Law Enforcement Cooperation. (2022). *FACING REALITY? LAW ENFORCEMENT AND THE CHALLENGE OF DEEPFAKES.* Luxembourg: Publications Office of the European Union.

European Union Agency for Law Enforcement Cooperation. (2022). *POLICING IN THE METAVERSE: WHAT LAW ENFORCEMENT NEEDS TO KNOW.* Luxembourg: Publications Office of the European Union.

European Union Agency for Law Enforcement Cooperation. (2023). *ChatGPT - The impact of Large Language Models.* Luxembourg: Publications Office of the European Union.

European Union Agency for Law Enforcement Cooperation. (2023). *Internet Organised Crime Threat Assessment.*

Khiralla, F. (2020). Statistics of cybercrime from 2016 to the first half of 2020. . *Int. J. Comput. Sci. Netw., 9(5*, 252-261.

Ministère public de la Confédération. (2021). *Rapport de gestion 2020.*

Ministère public de la Confédération. (2022). *Rapport de Gestion 2021.*

Office fédéral de la justice. (2021). *Rapport sur l'US CLOUD Act.*

Office fédéral de la justice. (2023). *Rapport sur le projet e-evidence de l'UE.*

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age.* Cambridge, Polity.

Annexes

1 Méthodologie du sondage

Le sondage a été établi par fedpol et le RNS, a été consolidé avec différents partenaires des polices cantonales (NEDIK via ZH, GE) ainsi que des ministères publics (MPC, CMP) et de la PSC. Le sondage comptait des questions générales et spécifiques (ne concernant respectivement que la police ou les ministères publics). Le sondage a ensuite été diffusé en février 2023 via la CCPCS, la CMP ainsi que via les chancelleries cantonales, respectivement aux corps de police, aux ministères publics ainsi qu'aux tribunaux. Un délai de réponse de deux mois a été fixé.

Au final, 74 sondages complets ont été reçus via l'outil (dont 2 doublons) et un sondage complet a également été transmis par courriel.

- La quasi-totalité des polices cantonales (sauf une) ont répondu au sondage ainsi qu'une police municipale.
- La quasi-totalité des ministères publics (sauf un) ont répondu au sondage ainsi que le Ministère public de la Confédération.
- Une majorité des tribunaux (18 via l'outil + 1 par courriel) ont répondu.
- Des organisations autres, telles que la PCS, ont également répondu au sondage.