Formation policière dans le domaine numérique : une stratégie à trois niveaux

Sami Hafsi
Chef de la police judiciaire,
Commandant de la Police neuchâteloise (dès le 1er janvier 2024)

Sébastien Jaquier
Doyen de l'Institut de lutte contre la criminalité économique (ILCE),
Haute école de gestion Arc
Haute école de Suisse Occidentale (HES-SO)

Résumé

Face aux défis que représente la formation en matière de lutte contre la cybercriminalité, un modèle d'acquisition des connaissances à trois niveaux a été mis sur pied. L'e-learning ISP *Cybercrime* (e-CC) destiné à l'ensemble des forces de l'ordre et le cours ISP pour enquêtrices et enquêteurs constituent une réponse adaptée aux deux premiers niveaux axés sur les besoins des policières et policiers généralistes. Pour les spécialistes, une matrice de compétences a été développée et mise en ligne sur la plateforme Cyberpie. Son rôle est de fournir une grille de lecture des formations cyber qui y sont proposées en tenant compte des compétences spécifiques aux métiers de police. Ce développement novateur offre une vue d'ensemble des formations en faisant le lien entre l'offre et les besoins. L'exercice met en lumière une nouvelle possibilité d'exploiter plus utilement les profils de compétences établis.

Une stratégie en matière de lutte contre la cybercriminalité

L'interconnexion croissante des informations et des services influence notre société et questionne les autorités de poursuite pénale. Le modèle des 5V (volume, vélocité, variété, véracité, valeur) souligne également à quel point les données ne sont plus ce qu'elles étaient et combien l'environnement numérique se complexifie. Les enquêtrices et enquêteurs, magistrat·e·s, expert·e·s, mais aussi les chercheuses et les chercheurs sont confronté·e·s à des défis de taille, dont le premier est certainement le maintien et le développement des compétences. Face à l'évolution exponentielle de ce phénomène, la formation des professionnel·le·s constitue en effet un enjeu crucial pour l'ensemble des acteurs de la chaine pénale, mais également pour les hautes écoles et universités qui doivent proposer des programmes modulaires et adaptés pour répondre aux exigences d'un public cible dont les besoins sont très hétérogènes.

Une décennie s'est écoulée depuis que les premiers jalons d'une stratégie de formation en matière de lutte contre la cybercriminalité ont été posés en Suisse. Rapidement, le constat suivant s'est imposé : la composante numérique est omniprésente dans l'activité policière, il est donc essentiel de proposer une formation correspondant à la réalité du terrain à l'ensemble des policières et policiers suisses.

L'approche privilégiée s'oriente vers un modèle à trois niveaux, dont le premier étage n'est autre que le socle de connaissances de base en matière de préservation des traces numériques pour l'ensemble des policières et policiers. Le niveau intermédiaire s'adresse aux enquêtrices et enquêteurs généralistes, dont les compétences d'investigation doivent aller au-delà de la simple préservation des traces. Le sommet de cette pyramide de compétences couvre quant à lui le monde très vaste des formations spécialisées qu'il serait naïf de concevoir comme un simple prolongement des deux premiers niveaux. C'est uniquement en imaginant une approche flexible et sur mesure dédiée aux spécialistes des cyberenquêtes, des cyberanalyses et de l'investigation numérique que nous apportons une réponse cohérente à la diversité des besoins.

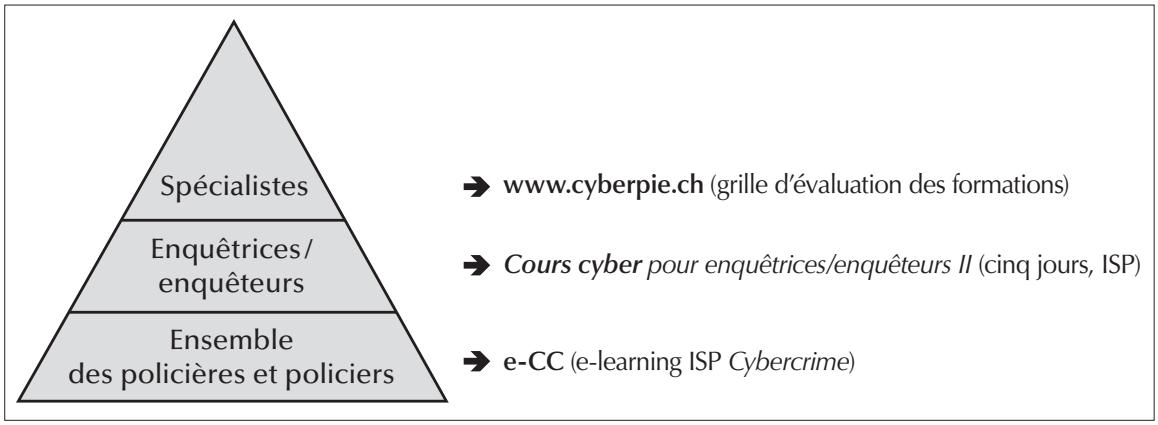

Figure 1 : Stratégie de formation à trois niveaux avec le public cible défini (à gauche) et la réponse proposée (à droite)

Afin d'élaborer une réponse adaptée pour les métiers des trois catégories mentionnées ci-dessus, une matrice a été mise sur pied au sein du groupe de travail national « Formation *Cybercrime* » mis en place par la Conférence des commandantes et des commandants des polices cantonales de Suisse (CCPCS). Validée par la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP), cette matrice définit le niveau de maitrise de cinq profils (métiers) pour treize domaines de compétences[1] et sert désormais de feuille de route à la mise en œuvre et au suivi de la stratégie globale de formation en matière numérique.

Formation de base : la police aux avant-postes

La formation policière intègre depuis de nombreuses années la composante numérique, aussi bien au niveau de la formation des aspirantes et aspirants que de la formation continue.

L'e-learning *Cybercrime* (e-CC) publié par l'Institut Suisse de Police (ISP) et hébergé sur la Plateforme nationale de formation policière (PNFP) est à disposition de l'ensemble des personnels de police. Cette formation en ligne a pour objectif principal de sensibiliser et former les policières et policiers, quelles que soient leurs missions, en matière de cybercriminalité et de préservation de la trace numérique. Issue d'une formation pilote menée en présentiel dès 2016, elle se décline sous la forme d'un e-learning depuis 2018. Son contenu est adapté au fil du temps en tenant compte de l'évolution des phénomènes criminels en particulier.

Cet outil fait à ce titre partie de la panoplie des ressources dont disposent les personnels des forces de police afin d'assurer la mise à jour de leurs connaissances pour le travail en première ligne. La formation e-CC s'inscrit pleinement dans la stratégie de formation policière en matière de lutte contre la cybercriminalité élaborée sous l'égide du groupe de travail « Formation *Cybercrime* ». Elle découle des besoins listés dans la matrice de compétences brièvement présentée précédemment pour le profil « Policière/policier de front ».

Cours intermédiaires pour enquêtrices et enquêteurs

Si l'ensemble des forces de police se doivent de disposer de connaissances minimales en matière de préservation de la trace numérique, c'est parce que la composante numérique est présente dans la plupart des infractions pénales.

C'est ce constat qui justifie le développement de compétences de base en matière d'enquête sur le terrain clé du numérique. Contrairement à l'e-learning e-CC, le *Cours cyber pour enquêtrices / enquêteurs* se déroule en présentiel et s'adresse à l'ensemble des enquêtrices et enquêteurs de police judiciaire. Cette formation, initiée en 2017 déjà et dispensée

Figure 2 : Page d'accueil de la formation e-CC

1 Par exemple : droit, protection des données, recherches sur internet, surveillance des télécommunications, analyse forensique de la téléphonie.

sous l'égide de l'ISP, est également coordonnée par le groupe de travail « Formation *Cybercrime* ». Elle se déroule dans les trois régions linguistiques avec, pour chaque région, une direction de cours et une direction technique pilotant une équipe d'intervenant·e·s spécialisé·e·s, en général issu·e·s des forces de police.

Il ne s'agit plus ici d'acquérir des connaissances de base en matière cyber, mais bien de développer un certain nombre de compétences au niveau de l'analyse et de l'exploitation de la trace numérique au service de l'enquête.

L'évaluation continue de la formation conduit à une revue périodique des contenus enseignés. Il s'agit de résoudre une équation aussi complexe qu'essentielle, à savoir développer des compétences en intégrant l'évolution de la menace et le développement de la pratique policière tout en tenant compte des compétences des participant·e·s.

Le *Cours cyber pour enquêtrices / enquêteurs* constitue la seconde étape de formation généraliste élaborée dans le cadre de la stratégie policière en matière de lutte contre la cybercriminalité.

CYBERPIE
Formations pour les polices

Formations spécifiques destinées aux spécialistes

L'investigation numérique, pour ne prendre que cet exemple, ne se résume pas à un champ étroit de compétences, mais touche un spectre extrêmement large de domaines tels que l'exploitation forensique des ordinateurs et supports de données, la téléphonie mobile, les systèmes embarqués, la surveillance des télécommunications, l'analyse ou encore l'engagement lié à un incident cyber. Ces compétences – aussi variées que spécifiques – touchent des activités qui sont elles-mêmes en constante évolution, si bien que leur maîtrise au fil du temps requiert une pratique intensive. Cette évolution explique que les spécialistes en investigation numérique se concentrent en principe sur un nombre limité de domaines. Il revient aux chef·fe·s de brigades d'investigation numérique ou aux responsables de la formation de constituer des équipes multidisciplinaires et complémentaires aptes à couvrir le spectre de ces domaines spécifiques. Partant du postulat qu'il n'est pas réaliste d'offrir une formation de pointe sur l'ensemble des treize domaines de compétences aux spécialistes en investigation numérique, en cyberanalyse et en cyberenquête, plusieurs initiatives ont été lancées en vue de se doter d'un recueil de formations. Le groupe de travail « Formation *Cybercrime* » est rapidement arrivé à la conclusion que l'offre de formation devait non seulement être regroupée au sein d'un seul et même recueil, mais qu'elle devait également répondre à des besoins spécifiques en termes de contenu, de langue, de durée, de compétences, de prix et de qualité. Il est également apparu que ce catalogue devait être évolutif, doté d'une capacité de tri et disponible en source ouverte. Ce dernier critère est important, car il agit sur deux niveaux. D'une part, il permet aux policières et policiers ainsi qu'aux responsables de la formation de construire un plan de formation solide et cohérent. D'autre part, il permet aux hautes écoles et universités de détecter les besoins et de mettre sur pied les formations adéquates en veillant à une certaine complémentarité entre les institutions de formation.[2]

Il ne s'agit plus ici d'acquérir des connaissances de base en matière cyber, mais bien de développer un certain nombre de compétences au niveau de l'analyse et de l'exploitation de la trace numérique au service de l'enquête.

Le groupe de travail « Formation *Cybercrime* » a ainsi conceptualisé puis réalisé un outil en ligne intégrant la matrice de compétences précitée pour les formations proposées par les institutions de formation spécialisées. De cette initiative est né le site internet https://cyberpie.edupolice.ch hébergé sur la Plateforme nationale de formation policière (PNFP). Ce site ambitionne de réunir les institutions de formations susceptibles de proposer des offres pertinentes, d'un côté, et les responsables de formation et personnels cherchant à se former, de l'autre. L'offre apparaît sous la forme d'une liste classée par ordre de pertinence.

La plateforme en ligne Cyberpie propose ainsi une lecture synthétique des contenus d'apprentissage des différentes formations au travers de la matrice de compétences liée au profil considéré. En d'autres termes, elle permet de déterminer dans quelle mesure une formation correspond au besoin et d'effectuer un tri de l'offre existante. L'intégration d'une fonctionnalité permettant l'évaluation des cours permet aux futur·e·s participant·e·s de tirer profit de l'expérience acquise par les volées précédentes.

2 Une étude finalisée en 2022 par le Réseau national de sécurité (RNS) a par exemple permis de réaliser un panorama des formations supérieures dans le domaine cyber en Suisse. Cette vue d'ensemble, même si elle n'ambitionne pas d'être exhaustive, a permis d'illustrer la richesse et la diversité de l'offre en la matière.

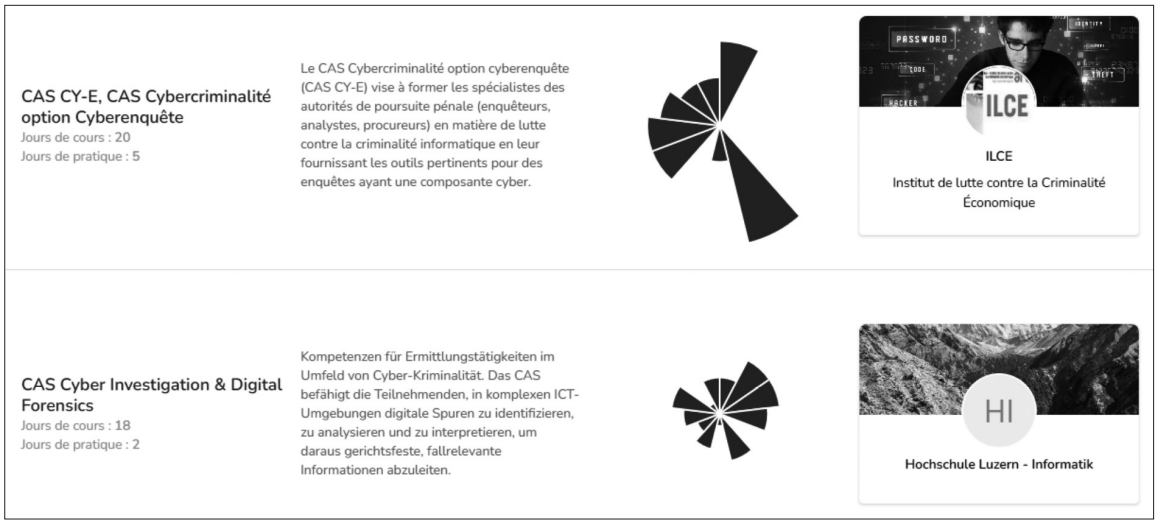

Figure 3 : Comparaison entre deux CAS pour cyberenquêtrices et cyberenquêteurs (source : https://cyberpie.edupolice.ch).

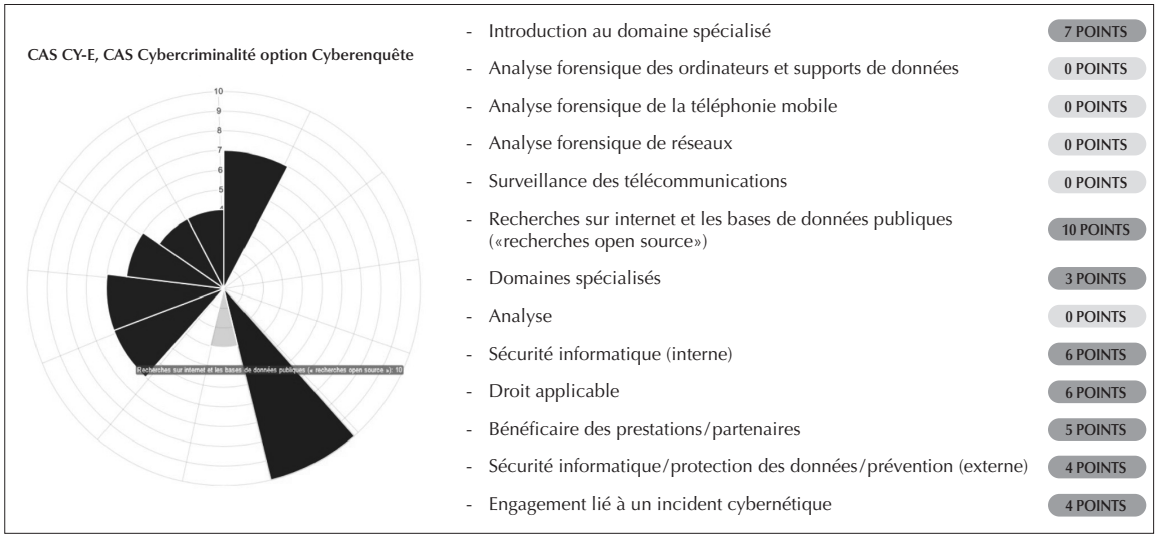

Figure 4 : Détail des matières enseignées dans le cadre d'une formation (source : https://cyberpie.edupolice.ch)

Un modèle innovant et inspirant

Si les cybercriminel·le·s font preuve d'une créativité débordante, les forces de l'ordre doivent également faire preuve de dynamisme et d'une grande capacité d'adaptation. C'est en mettant en place une structure de formation adaptée qu'elles y parviendront. La formation en matière cyber nécessite un cadre permettant à chaque policière et policier d'appréhender le vaste éventail des situations dans lesquelles ces technologies sont impliquées. Telle est la conséquence de l'évolution permanente des besoins et de la complexité de l'environnement dans le domaine.

L'intégration de plusieurs profils de compétences au sein d'une matrice destinée tant à la police qu'aux institutions de formation peut être considérée comme une solution innovante dans le paysage national.

L'intégration de plusieurs profils de compétences au sein d'une matrice destinée tant à la police qu'aux institutions de formation peut être considérée comme une solution innovante dans le paysage national. Cette mise en commun d'informations présente de multiples avantages qui peuvent être classés en trois groupes. Premièrement, les responsables de la formation peuvent s'appuyer sur un outil qui offre une base d'orientation et de décision claire. Deuxièmement, le personnel à former acquiert une vue synthétique et pertinente de l'offre connue, triée et potentiellement évaluée par d'ancien·ne·s participant·e·s. Finalement, les instituts et écoles bénéficient d'une plateforme permettant de mettre en valeur leur offre d'une part et de la construire ou de la compléter d'autre part.

Le projet Cyberpie démontre que l'on peut tirer plus de bénéfice des profils de compétences mis sur pied lorsqu'ils sont intégrés à un outil qui les rend concrets. Ce modèle pourrait être bénéfique à d'autres champs d'activités lorsque la complexité des formations et des besoins rend l'offre difficilement lisible.

Zusammenfassung

Polizeiausbildung für den Cyberspace: Eine dreistufige Strategie

Ausbildung und Training im Bereich der Bekämpfung von Cyberkriminalität sind ein eigenes Gebiet. Angesichts der damit verbundenen Herausforderungen wurde ein dreistufiges Lernmodell konzipiert. Das E-Learning *Cybercrime* (e-CC) des SPI, das allen Angehörigen der Polizei offensteht, und der SPI-Kurs für Ermittlerinnen und Ermittler sind eine Antwort auf die ersten zwei Stufen, die sich den Bedürfnissen von Polizistinnen und Polizisten ohne Spezialisierung widmen. Für Spezialistinnen und Spezialisten hingegen wurde eine Kompetenzmatrix erstellt, die auf der Plattform *CyberPie* online zugänglich ist. Sie bietet eine Übersicht über alle auf der Plattform verfügbaren Cyber-Kurse unter Berücksichtigung polizeispezifischer Kompetenzen. So werden Kursangebot und Schulungsbedarf auf innovative Weise zusammengeführt und übersichtlich dargestellt. Dieser Ansatz richtet den Fokus darauf, wie sich die erstellten Kompetenzprofile besser nutzen lassen.

Riassunto

Formazione di polizia in ambito digitale: una strategia a tre livelli

Di fronte alle sfide della formazione in materia di lotta alla cybercriminalità è stato creato un modello a tre livelli sull'acquisizione delle conoscenze. L'e-learning ISP *Cybercrime* (e-CC), destinato a tutte le forze dell'ordine, e i corsi ISP per inquirenti costituiscono una risposta adeguata ai due primi livelli, basati sulle esigenze degli agenti di polizia generalisti. Per gli specialisti è stata invece sviluppata un'apposita matrice di competenze, che è stata poi pubblicata online sulla piattaforma Cyberpie. Il suo scopo consiste nel fornire una griglia di lettura delle formazioni proposte su Cyberpie tenendo in considerazione le competenze specifiche dei mestieri di polizia. Questo sviluppo innovatore offre una visione d'insieme sulle formazioni e collega al contempo domanda e offerta. L'esercizio mette in luce una nuova possibilità di sfruttare al meglio i profili di competenze.