EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Audit de l'efficacité de la lutte contre la cybercriminalité

Office fédéral de la police

CDF-19394 | Prises de position incluses | 1er mars 2021 | DélFin D2/2021

Bestelladresse Adresse de commande Indirizzo di ordinazione Ordering address	Contrôle fédéral des finances (CDF) Monbijoustrasse 45 3003 Berne Suisse
Bestellnummer Numéro de commande Numero di ordinazione Ordering number	1.19394.403.00133
Zusätzliche Informationen Complément d'informations Informazioni complementari Additional information	www.efk.admin.ch info@efk.admin.ch twitter: @EFK_CDF_SFAO + 41 58 463 11 11
Abdruck Reproduction Riproduzione Reprint	Gestattet (mit Quellenvermerk) Autorisée (merci de mentionner la source) Autorizzata (indicare la fonte) Authorized (please mention source)

Sauf indication contraire, les dénominations de fonction dans ce rapport s'entendent aussi bien à la forme masculine que féminine.

Table des matières

Audit de l'efficacité de la lutte contre la cybercriminalité
Office fédéral de la police

L'essentiel en bref

La criminalité numérique a des limites floues, des initiateurs incernables et souvent une dimension internationale. C'est un défi pour les autorités de poursuite pénale. Dans neuf cas sur dix, ces crimes relèvent de la compétence cantonale. Toutefois, l'Office fédéral de la police (fedpol) est essentiel dans cette lutte : comme office central et point de contact international, il apporte son aide aux polices des cantons. De plus, fedpol soutient le Ministère public de la Confédération (MPC) dans ses procédures de cybercrminalité complexe de compétence fédérale.

Le Contrôle fédéral des finances (CDF) a audité l'efficacité de la lutte contre la cybercriminalité chez fedpol. Il s'est rendu en Argovie, à Berne, dans le canton de Vaud, au Tessin et à Zoug ainsi qu'au MPC pour saisir l'environnement dans lequel fedpol évolue et la perception de ses partenaires. Les services de la Police judiciaire fédérale (PJF) – de sa division « IT Forensique & CyberCrime » (IFC) et de sa division « Criminalité économique » – sont appréciés par les cantons et le MPC. La lutte contre la pédocriminalité en ligne fait l'objet de clarifications entre les cantons et la Confédération. Le CDF identifie pourtant des pistes pour améliorer l'efficacité du suivi des affaires de la PJF, ses capacités d'analyse et sa coopération avec le MPC.

Adéquation des ressources chez fedpol et prestations jugées bonnes par les cantons

L'analyse d'un échantillon de dossiers personnels de l'IFC note une adéquation entre les compétences des employés et leurs tâches, même si des différences existent selon les fonctions. Le CDF voit un risque de démotivation chez les collaborateurs de l'IFC arrivés il y a peu et/ou avec des formations pointues en raison d'une progression salariale à l'ancienneté.

Les cantons vus par le CDF apprécient les prestations de l'IFC et son aide dans la coopération internationale. Faute de ressources, ces cantons identifient un besoin d'analyse de la cybercriminalité que fedpol pourrait développer à l'avenir. De plus, l'IFC trie aussi les annonces d'images interdites émises par ses partenaires – tel le National Center for Missing and Exploited Children – et les dénonce aux cantons. Pour le CDF et en application du cadre légal actuel, fedpol devrait améliorer le suivi de ces dénonciations auprès de ses partenaires cantonaux.

Collaboration et divergences avec le MPC, centralisation opportune des achats sur le plan fédéral

Avec fedpol, la sous-division Cyber du MPC mène des procédures de cybercriminalité complexes. Elle collabore sans difficulté majeure avec la PJF. Mais, le MPC et fedpol divergent sur la création d'un « cyber-commissariat » à la PJF, comme correspondant à la sous-division Cyber du MPC. Pour plus d'efficacité, ces autorités se sont réorganisées depuis dix ans et ont fait correspondre leurs structures (« effet miroir »). Or, ce n'est plus le cas avec la création de la sous-division Cyber au MPC fin 2019. A cette occasion, la communication entre ces autorités n'a pas non plus été optimale. Le CDF recommande à fedpol d'analyser les avantages et les inconvénients d'un « cyber-commissariat » à la PJF ou de toute autre solution pour assurer la disponibilité des ressources aux procédures pénales « cyber » du MPC d'ici juillet 2021.

Les entités fédérales – dont fedpol et le MPC – et les cantons dépensent plusieurs millions de francs par an en prestations forensiques IT auprès d'une seule société. Celle-ci réalise près de

80 % de son chiffre d'affaires avec le secteur public. Le CDF recommande à fedpol d'établir un centre de compétences, notamment forensiques, pour l'administration fédérale, et ainsi centraliser les besoins pour apporter une réponse économe et efficace dans ce domaine.

Environnement applicatif et traitement numérique des dossiers à renforcer en priorité

A l'IFC et à la PJF, le traitement numérique des données d'enquête n'est pas sans risques. La direction de fedpol a identifié cela début 2019. La situation devrait être améliorée via le programme « Ermittlungssystem » (ErmSys) avec une échéance ambitieuse en 2022. Le CDF recommande à fedpol de rendre prioritaire le programme ErmSys pour assurer un cadre de travail adéquat, sûr, assurant la traçabilité des informations pour les partenaires fédéraux et cantonaux de la PJF et donnant un support de travail efficace à ses équipes.

Sans outils performants et automatisés de pilotage, la PJF s'expose à un risque de conduite insuffisamment structurée des dossiers, limitant sa marge de manœuvre et l'anticipation des problèmes. Ces difficultés s'illustrent dans l'analyse d'environ 170 dossiers de *phishing* (hameçonnage de données). Sollicitée par le MPC en 2017, cette analyse a pris fin en octobre 2020. Le MPC attend encore la livraison des rapports de police. A l'avenir, la PJF prévoit la création d'un monitoring moderne intégré dans les améliorations envisagées par fedpol. Le CDF recommande à fedpol de renforcer les outils de pilotage des activités de la PJF grâce un monitoring (cockpit et indicateurs) pour la gestion des dossiers, y compris le suivi des dénonciations de fedpol aux cantons (images interdites).

Clarifications bienvenues dans la lutte contre la pédocriminalité numérique

Fin 2019, le Parlement a octroyé quatre postes à fedpol pour la cyber-pédocriminalité. Les documents reçus par le CDF montrent une traçabilité partielle lors de la création de ces postes, dont deux hors PJF. Ils ne permettent pas de dire si fedpol a respecté ou non la volonté du Parlement. Le CDF lui recommande d'examiner et de justifier l'allocation des postes afin que la décision du Parlement et les besoins exprimés par les cantons puissent être satisfaits.

La pédocriminalité numérique est de compétence cantonale. Depuis 2001, fedpol réalise toutefois des recherches actives contre cette criminalité au profit des cantons. Ici, le CDF a constaté un arrêt durant neuf mois en 2018 des enquêtes sous couverture contre les cyber-pédophiles. Dès le 1er janvier 2021, ces recherches actives iront désormais aux cantons selon une convention entre la Conférence des directrices et directeurs des départements cantonaux de justice et police et la Conférence des Commandants des Polices Cantonales de Suisse. La mise en œuvre incombe aux cantons dont les ressources pour relever ce défi se construisent. Pour le CDF, cette clarification du travail entre fedpol et les cantons est opportune.

Des indicateurs de performance pour la Stratégie nationale de protection contre les cyberrisques

Le CDF a audité le volet pénal de la Stratégie nationale de protection contre les cyberrisques (SNPC II) et la mise en œuvre des mesures relatives. Le Centre national pour la cybersécurité (NCSC) coordonne ces activités et effectue un contrôle de gestion stratégique. Il admet que des risques en matière pénale ne sont pas entièrement couverts. Ces risques font cependant l'objet d'un processus d'appréciation pour évaluer de nouvelles mesures à prendre.

Pour lutter contre la cybercriminalité, les mesures de la SNPC II à appliquer ont un caractère général et leurs calendriers mériteraient d'être précisés. Le NCSC ne dispose pas d'un monitoring critique de leur mise en œuvre. Pour une future SNPC III, le CDF recommande d'élaborer un système d'indicateurs de performance afin d'évaluer la réalisation des objectifs à atteindre pour chaque mesure.

Wirksamkeitsprüfung der Bekämpfung von Cyberkriminalität

Bundesamt für Polizei

Das Wesentliche in Kürze

Die Grenzen der Cyberkriminalität sind unscharf, ihre Urheber schwer zu fassen, zudem weist diese Form von Kriminalität oft eine internationale Dimension auf. Dies stellt die Strafverfolgungsbehörden vor grosse Herausforderungen. Die Straftaten fallen in neun von zehn Fällen in die Zuständigkeit der Kantone. Das Bundesamt für Polizei (fedpol) spielt jedoch eine entscheidende Rolle bei diesem Kampf: als zentrales Bundesamt und als internationale Kontaktstelle unterstützt es die Kantonspolizeien bei ihrer Arbeit. Das fedpol hilft auch der Bundesanwaltschaft (BA) in ihren komplexen Verfahren gegen Cyberkriminalität, für die der Bund zuständig ist.

Die Eidgenössische Finanzkontrolle (EFK) hat die Wirksamkeit der Bekämpfung der Cyberkriminalität durch die fedpol geprüft. Sie ist in die Kantone Aargau, Bern, Waadt, Tessin und Zug gegangen und hat die BA besucht, um das Umfeld, in dem das fedpol tätig ist und die Einschätzung seiner Partner zu sondieren. Die Dienste der Bundeskriminalpolizei (BKP) – ihrer Abteilungen «IT-Forensik, Cybercrime» (IFC) und «Wirtschaftskriminalität» – werden von den Kantonen und der BA geschätzt. Die Bekämpfung der Pädokriminalität im Internet ist Gegenstand von Abklärungen zwischen dem Bund und den Kantonen. Die EFK sieht jedoch Möglichkeiten, die Effizienz in der Nachverfolgung der Dossiers der BKP, ihre Analysekapazitäten und Zusammenarbeit mit der BA zu verbessern.

Angemessenheit der Ressourcen des fedpol und gute Bewertung seiner Leistungen durch die Kantone

Eine Stichprobenanalyse von Personaldossiers der IFC zeigt, dass die Kompetenzen der Mitarbeitenden ihren Aufgaben entsprechen, auch wenn es Unterschiede zwischen den einzelnen Funktionen gibt. Bei den erst vor Kurzem eingetretenen und/oder hochqualifizierten Mitarbeitenden stellt die EFK ein Risiko der Demotivierung fest, das in der dienstaltersabhängigen Lohnentwicklung gründet.

Die Kantone, die von der EFK befragt wurden, schätzen die Dienstleistungen der IFC und ihre Unterstützung in der internationalen Zusammenarbeit. Aufgrund von fehlenden Ressourcen erkennen die Kantone einen Bedarf an Analysen zur Cyberkriminalität, den das fedpol in Zukunft ausbauen könnte. Die Abteilung IFC sortiert ausserdem die Meldungen ihrer Partner – z. B. das National Center for Missing and Exploited Children (NCMEC) – über verbotenes Bildmaterial und erhebt bei den Kantonen Anzeige. Der EFK zufolge und unter Anwendung des geltenden Rechtsrahmens sollte das fedpol die Nachverfolgung dieser Meldungen bei seinen kantonalen Partnern verbessern.

Zusammenarbeit und Meinungsverschiedenheiten mit der BA, zweckmässige Zentralisierung der Beschaffungen auf Bundesebene

Die Unterabteilung Cyberkriminalität der BA führt zusammen mit dem fedpol komplexe Cyberkriminalitätsverfahren durch. Die Zusammenarbeit mit der BKP gestaltet sich weitgehend problemlos. Uneinigkeit besteht jedoch zwischen der BA und fedpol hinsichtlich der Schaffung eines «Cyber-Kommissariats» bei der BKP als Pendant zur Unterabteilung Cyberkriminalität bei der BA. Die beiden Behörden haben vor zehn Jahren begonnen, sich zwecks grösserer Effizienz neu zu organisieren und ihre Strukturen («spiegelbildlich») anzugleichen. Mit der Schaffung der Unterabteilung Cyberkriminalität bei der BA Ende 2019 war dies jedoch nicht mehr der Fall. Auch die Kommunikation zwischen beiden Behörden verlief nicht optimal. Die EFK empfiehlt dem fedpol, die Vor- und Nachteile eines «Cyber-Kommissariats» in der BKP oder einer anderen Lösung zu analysieren, um die Verfügbarkeit von Ressourcen für «Cyberkriminalitätsstrafverfahren» der BA ab Juli 2021 sicherzustellen.

Die Bundesstellen – unter anderem das fedpol und die BA – und die Kantone geben jedes Jahr mehrere Millionen Franken für forensische IT-Leistungen aus, die sie bei ein- und demselben Unternehmen beziehen. Dieses Unternehmen erzielt knapp 80 % seines Umsatzes mit dem öffentlichen Sektor. Die EFK empfiehlt dem fedpol, ein Kompetenzzentrum, insbesondere im Bereich der Forensik, für die Bundesverwaltung zu schaffen, um so den Bedarf zu bündeln und in diesem Bereich eine wirtschaftliche und wirksame Lösung zu finden.

Anwendungsumgebung und digitale Dossierbearbeitung als prioritäre Anliegen

Die digitale Bearbeitung von Erhebungsdaten in der IFC und der BKP ist nicht ohne Risiken. Die Direktion des fedpol hat dies bereits Anfang 2019 erkannt. Die Situation sollte mithilfe des Programms «Ermittlungssystem» (ErmSys) mit einer ehrgeizigen Frist bis 2022 verbessert werden. Die EFK empfiehlt dem fedpol, dem Programm ErmSys Priorität einzuräumen, um eine angemessene und sichere Arbeitsumgebung zu schaffen, die für die Partner der BKP beim Bund und bei den Kantonen die Nachverfolgbarkeit der Informationen gewährleistet und ihren Teams eine effiziente Arbeitshilfe gibt.

Ohne leistungsstarke und automatisierte Steuerungstools setzt sich die BKP dem Risiko einer ungenügend strukturierten Dossierverwaltung aus, die ihren Handlungsspielraum und die frühzeitige Erkennung von Problemen einschränkt. Diese Schwierigkeiten werden in der Analyse von rund 170 *Phishing-Dossiers* (Datenraub) deutlich. Die 2017 von der BA angeforderte Analyse wurde im Oktober 2020 abgeschlossen. Die BA wartet immer noch auf die Polizeiberichte. In Zukunft sieht die BKP die Schaffung eines modernen Monitorings vor, das in die vom fedpol geplanten Verbesserungen integriert ist. Die EFK empfiehlt dem fedpol, die Instrumente zur Steuerung der Aktivitäten der BKP durch ein Monitoring (Cockpit und Kennzahlen) für die Dossierverwaltung, einschliesslich der Nachverfolgung der Meldungen vom fedpol an die Kantone (verbotenes Bildmaterial), zu stärken.

Willkommene Klärungen bei der Bekämpfung der Pädokriminalität im Netz

Ende 2019 bewilligte das Parlament dem fedpol vier neue Stellen im Bereich Cyber-Pädokriminalität. Die der EFK ausgehändigten Dokumente zeigen eine teilweise Rückverfolgbarkeit bei der Schaffung dieser Stellen, von denen zwei nicht zur BKP gehören. Es lässt sich aufgrund dieser Unterlagen nicht sagen, ob das fedpol den Willen des Parlaments respektiert hat oder nicht. Die EFK empfiehlt dem fedpol, die Zuteilung der Stellen zu überprüfen und zu begründen, damit dem Entscheid des Parlaments Folge gegeben und der von den Kantonen angemeldete Bedarf erfüllt werden kann.

Die Pädokriminalität im Netz fällt in die Zuständigkeit der Kantone. Seit 2001 führt jedoch das fedpol aktiv Ermittlungen gegen diese Form der Kriminalität zugunsten der Kantone durch. In diesem Bereich hat die EFK im Jahr 2018 einen neunmonatigen Unterbruch der verdeckten Ermittlungen gegen Cyber-Pädophile festgestellt. Seit dem 1. Januar 2021 übernehmen gemäss einer Vereinbarung zwischen der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren und der Konferenz der Kantonalen Polizeikommandanten der Schweiz die Kantone diese aktiven Ermittlungen. Die Umsetzung der Vereinbarung obliegt den Kantonen, die daran sind, Ressourcen für die Erfüllung dieser Aufgabe aufzubauen. Die EFK erachtet diese Klarstellung der Aufgabenteilung zwischen dem fedpol und den Kantonen als willkommen.

Leistungsindikatoren für die nationale Strategie zum Schutz vor Cyberrisiken

Die EFK hat den strafrechtlichen Teil der nationalen Strategie zum Schutz vor Cyberrisiken (NCS II) und die Umsetzung der entsprechenden Massnahmen geprüft. Das Nationale Zentrum für Cybersicherheit (NCSC) koordiniert die Aktivitäten und nimmt ein strategisches Controlling vor. Das NCSC anerkennt, dass gewisse strafrechtliche Risiken nicht vollständig abgedeckt sind. Diese Risiken werden aber einem Beurteilungsprozess unterzogen, um weitere Massnahmen zu evaluieren.

Die Massnahmen der NCS II zur Bekämpfung der Cyberkriminalität sind allgemeiner Natur, beim Zeitplan besteht Präzisierungsbedarf. Das NCSC überwacht die Umsetzung dieser Massnahmen nicht kritisch. Im Hinblick auf eine zukünftige NCS III empfiehlt die EFK, ein System von Leistungsindikatoren zu erarbeiten, um die Erreichung der Ziele für jede Massnahme zu bewerten.

Originaltext auf Französisch

Verifica dell'efficacia della lotta contro la cibercriminalità
Ufficio federale di polizia

L'essenziale in breve

La criminalità digitale ha contorni sfumati, iniziatori sfuggenti e si muove spesso in un contesto internazionale. Ciò rappresenta una sfida per le autorità di perseguimento penale. In nove casi su dieci, questo reato rientra nella competenza dei Cantoni. Tuttavia, l'Ufficio federale di polizia (fedpol), in qualità di ufficio centrale e punto di contatto internazionale, svolge un ruolo essenziale in questo ambito, supportando le forze di polizia cantonali. Inoltre, fedpol sostiene il Ministero pubblico della Confederazione (MPC) nei procedimenti relativi a casi di cibercriminalità complessa di competenza federale.

Il Controllo federale delle finanze (CDF) ha verificato l'efficacia della lotta contro la cibercriminalità da parte di fedpol. Il CDF si è recato nei Cantoni di Argovia, Berna, Vaud, Ticino e Zugo, così come presso il MPC per analizzare l'ambiente in cui fedpol opera e quale ne sia la percezione da parte dei partner. I servizi della Polizia giudiziaria federale (PGF), delle sue divisioni «Informatica forense, cibercriminalità» (IFC) e «Criminalità economica», sono apprezzati dai Cantoni e dal MPC. La lotta contro la pedocriminalità in Internet è oggetto di chiarimenti tra i Cantoni e la Confederazione. Tuttavia, il CDF sta valutando soluzioni per migliorare l'efficacia del monitoraggio dei casi della PGF, delle sue capacità di analisi e della sua collaborazione con il MPC.

Adeguatezza delle risorse di fedpol e valutazione positiva delle prestazioni da parte dei Cantoni

L'analisi di un campione di dossier personali dell'IFC rileva corrispondenza tra le competenze dei collaboratori e i loro compiti, sebbene esistano discrepanze a seconda delle funzioni. Il CDF ravvisa nell'evoluzione dello stipendio basata sull'anzianità un rischio di demotivazione tra i collaboratori dell'IFC di recente assunzione e/o con una formazione avanzata.

I Cantoni esaminati dal CDF apprezzano le prestazioni dell'IFC e il supporto da questa fornito nella cooperazione internazionale. In mancanza di risorse, questi Cantoni rilevano un fabbisogno di analisi della cibercriminalità che fedpol potrebbe sviluppare in futuro. Inoltre, l'IFC seleziona le segnalazioni di immagini vietate emesse dai suoi partner, tra cui il «National Center for Missing and Exploited Children», e le trasmette ai Cantoni. Secondo il CDF, fedpol dovrebbe migliorare il monitoraggio di tali denunce presso i suoi partner cantonali, conformemente alle norme vigenti.

Collaborazione e divergenze con il MPC, centralizzazione opportuna degli acquisti a livello federale

Insieme a fedpol, la sottodivisione Cyber del MPC esegue procedure complesse di cibercriminalità. Questa sottodivisione collabora con la PGF senza particolari difficoltà. Tuttavia, il MPC e fedpol non concordano in merito alla creazione di un «cibercommissariato» presso la PGF quale unità omologa della sottodivisione Cyber del MPC. Per una maggiore efficacia, negli ultimi dieci anni queste autorità si sono riorganizzate creando strutture speculari. Ciò è cambiato con l'introduzione della sottodivisione Cyber nel MPC, a fine 2019. In tale occasione, anche la comunicazione tra queste autorità non è stata ottimale. Il CDF raccomanda

a fedpol di analizzare i vantaggi e gli svantaggi di un «cibercommissariato» presso la PGF o di qualsiasi altra soluzione per garantire entro luglio 2021 la disponibilità delle risorse necessarie per i procedimenti penali del MPC relativi a casi di cibercriminalità.

I servizi federali, tra cui fedpol e il MPC, e i Cantoni stanziano diversi milioni di franchi all'anno per le prestazioni di informatica forense di un'unica società. Questa società realizza circa l'80 per cento del suo fatturato con il settore pubblico. Il CDF raccomanda a fedpol di istituire un centro di competenza per l'Amministrazione federale, in particolare nel settore forense, e centralizzare così il fabbisogno, al fine di fornire una risposta economica ed efficace in questo ambito.

Priorità al rafforzamento dell'ambiente informatico e del trattamento digitale dei dossier

Presso l'IFC e la PGF il trattamento digitale dei dati relativi alle indagini non è privo di rischi. La direzione di fedpol ha individuato tale problematica a inizio 2019. Grazie al programma «Ermittlungssystem» (ErmSys), la situazione dovrebbe migliorare, con una scadenza ambiziosa, già nel 2022. Il CDF raccomanda a fedpol di dare la priorità a ErmSys, al fine di garantire un contesto di lavoro adeguato, sicuro e in grado di assicurare ai partner federali e cantonali della PGF la tracciabilità delle informazioni, così come di offrire un supporto efficace al lavoro svolto dai team.

Senza strumenti di gestione efficienti e automatizzati, la PGF si espone al rischio di una gestione dei dossier non sufficientemente strutturata, limitando di conseguenza il proprio margine di manovra e la capacità di anticipare i problemi. Queste difficoltà si riscontrano nell'analisi di circa 170 casi di *phishing*. Richiesta dal MPC nel 2017, l'analisi è stata completata nell'ottobre 2020. Attualmente il MPC sta attendendo la consegna dei rapporti di polizia. In futuro, la PGF prevede la creazione di un moderno sistema di monitoraggio come parte integrante dei miglioramenti previsti da fedpol. Il CDF raccomanda a fedpol di rafforzare gli strumenti di gestione delle attività svolte dalla PGF attraverso un sistema di monitoraggio (cockpit e indicatori) per la gestione dei dossier, compreso il follow-up delle denunce di fedpol ai Cantoni (immagini vietate).

Chiarimenti auspicati nella lotta contro la pedocriminalità digitale

A fine 2019 il Parlamento ha assegnato quattro posti a fedpol da impiegare nella lotta contro la pedocriminalità in Internet. La documentazione presentata al CDF mostra una tracciabilità parziale nella creazione di tali posti, due dei quali sono esterni alla PGF. Dai documenti non si evince se fedpol abbia rispettato o no la volontà del Parlamento. Il CDF raccomanda a fedpol di esaminare e giustificare l'assegnazione dei posti, affinché la decisione del Parlamento e il fabbisogno dei Cantoni siano rispettati.

La pedocriminalità digitale è di competenza cantonale. Tuttavia, dal 2001 fedpol ha indagato attivamente su questo reato per conto dei Cantoni. Al riguardo, ha constatato che nel 2018 le indagini sotto copertura contro i ciberpedofili sono state interrotte per nove mesi. Il 1° gennaio 2021 queste indagini attive sono state trasferite ai Cantoni in base a un accordo tra la Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia e la Conferenza dei comandanti delle polizie cantonali della Svizzera. L'attuazione spetta ai Cantoni, le cui risorse per affrontare questo compito sono in fase di implementazione. Il CDF ritiene opportuno chiarire i ruoli di fedpol e dei Cantoni.

Indicatori di prestazione concernenti la Strategia nazionale per la protezione contro i ciber-rischi

Il CDF ha verificato l'aspetto penale della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC II) e l'attuazione delle relative misure. Il Centro nazionale per la cibersicurezza (NCSC) coordina queste attività e svolge un controllo strategico della gestione. L'NCSC riconosce la presenza di rischi in materia penale non completamente coperti. Questi rischi vengono valutati al fine di considerare ulteriori misure da adottare.

Le misure della SNPC II da applicare nella lotta alla cibercriminalità hanno carattere generale e la loro tempistica necessita di una precisazione. L'NCSC non dispone di un monitoraggio critico dell'attuazione di tali misure. Nell'ottica di una futura SNPC III, il CDF raccomanda di sviluppare un sistema di indicatori di prestazione per valutare il raggiungimento degli obiettivi relativi a ogni misura.

Testo originale in francese

Audit of the effectiveness of the fight against cybercrime

Federal Office of Police

Key facts

Digital crime has fluid boundaries, elusive perpetrators and often involves an international dimension. It represents a challenge for the prosecution authorities. In nine out of ten cases, these crimes fall under cantonal jurisdiction. However, the Federal Office of Police (fedpol) plays an important role in this fight: as the central office and international contact point, it supports the cantonal police forces. In addition, fedpol supports the Office of the Attorney General of Switzerland (OAG) in complex cybercrime proceedings under federal jurisdiction.

The Swiss Federal Audit Office (SFAO) audited the effectiveness of fedpol's fight against cybercrime. The SFAO visited the cantons of Aargau, Bern, Vaud, Ticino and Zug as well as the OAG to gain an insight into the environment in which fedpol operates and the views of its partners. The services of the Federal Criminal Police (FCP) – its Forensic IT & Cybercrime Division and its Economic Crime Division – are appreciated by the cantons and the OAG. The fight against online paedophlia is still under discussion between the cantons and the Confederation. However, the SFAO identified ways to improve the efficiency of the FCP's case management, its analytical capabilities and its cooperation with the OAG.

Adequate resources at fedpol and good marks from the cantons for its services

The analysis of a sample of the Forensic IT & Cybercrime Division's personnel files shows that employees' skills are in line with their tasks, although there are differences depending on the role. The SFAO sees a risk of demotivation among Forensic IT & Cybercrime Division employees who have only recently joined the organisation and/or have specialised training, due to the fact that salary progression is based on seniority.

The cantons which the SFAO visited appreciated the Forensic IT & Cybercrime Division's services and its assistance in international cooperation. Due to a lack of resources, these cantons identified a need for cybercrime analyses that fedpol could develop in the future. In addition, the Forensic IT & Cybercrime Division also screens the reports of prohibited images submitted by its partners – such as the National Center for Missing and Exploited Children – and refers them to the cantons. In the SFAO's view, under the current legal framework, fedpol should improve its follow-up of these referrals to its cantonal partners.

Cooperation and differences with the OAG, appropriate centralisation of procurement at the federal level

Together with fedpol, the OAG's Cybercrime Sub-Division handles complex cybercrime cases. It cooperates with the FCP without any significant problems. However, the OAG and fedpol disagree on the creation of a "cyber office" within the FCP, as a counterpart to the OAG's Cybercrime Sub-Division. To increase efficiency, these authorities reorganised themselves over the last ten years and aligned their structures ("mirror effect"). However, this ceased to be the case with the creation of the OAG's Cybercrime Sub-Division at the end of

2019. Communication between these authorities was not optimal either. The SFAO recommends that fedpol analyse the advantages and disadvantages of a "cyber office" at the FCP or any other solution to ensure the availability of resources for the OAG's cybercriminal proceedings by July 2021.

The federal entities – including fedpol and the OAG – and the cantons spend several million francs a year on forensic IT services from a single company. This company generates around 80% of its turnover from the public sector. The SFAO recommends that fedpol establish a competence centre for the Federal Administration, especially in the area of forensics, and thus centralise the needs to provide a cost-effective and efficient response in this field.

Priority should be given to strengthening the application environment and digital processing of files

At the Forensic IT & Cybercrime Division and the FCP, the digital processing of investigation data is not without risks. Fedpol management identified this at the beginning of 2019. The situation should be improved through the investigation system (ErmSys) programme, which has an ambitious deadline of 2022. The SFAO recommends that fedpol prioritise the ErmSys programme in order to ensure an adequate, secure framework for the traceability of information for the FCP's federal and cantonal partners and to provide effective support for its teams.

Without efficient and automated management tools, the FCP is exposed to the risk of insufficiently structured case management, limiting its room for manoeuvre and anticipation of problems. These difficulties are illustrated by the analysis of around 170 phishing cases. This analysis was requested by the OAG in 2017 and was completed in October 2020. The OAG is still waiting for the delivery of the police reports. In the future, the FCP plans to create a modern monitoring system as part of the improvements planned by fedpol. The SFAO recommends that fedpol strengthen the tools for steering the FCP's activities by means of a monitoring system (cockpit and indicators) for case management, including the follow-up of fedpol's reports to the cantons (prohibited images).

Clarifications welcome in the fight against online paedophilia

At the end of 2019, Parliament allocated four posts to fedpol for internet paedophilia. The documents received by the SFAO show partial traceability in the creation of these positions, two of which were not within the FCP. It is not clear from the documents whether or not fedpol complied with Parliament's wishes. The SFAO recommends that fedpol examine and justify the allocation of posts so that the parliamentary decision and the needs expressed by the cantons can be met.

Online pedophilia falls under the jurisdiction of the cantons. Since 2001, however, fedpol has been actively investigating this crime on behalf of the cantons. The SFAO found that undercover investigations against paedophiles on the internet were paused for nine months in 2018. With effect from 1 January 2021, these active investigations were transferred to the cantons under an agreement between the Conference of Cantonal Justice and Police Directors and the Conference of Cantonal Police Commanders of Switzerland. Implementation is the responsibility of the cantons, whose resources to meet this challenge are being developed. The SFAO welcomes this clarification of the work done by fedpol and the cantons.

Performance indicators for the national strategy for the protection against cyber-risks

The SFAO audited the criminal law component of the national strategy for the protection of Switzerland against cyber-risks (NCS II) and the implementation of the related measures. The National Cybersecurity Centre (NCSC) coordinates these activities and carries out strategic management control. It recognises that there are risks in relation to criminal matters that are not fully covered. However, these risks are subject to an assessment process to evaluate what further measures should be taken.

The NCS II measures to be implemented to combat cybercrime are of a general nature and their timetables need to be clarified. The NCSC does not critically monitor their implementation. For a future NCS III, the SFAO recommends that a system of performance indicators be developed to assess whether the objectives of each measure have been achieved.

Original text in French

Prise de position générale des audités

Prise de position générale de fedpol

fedpol remercie le CDF pour le travail effectué dans le cadre de l'audit sur la lutte contre la cybercriminalité. De nombreux échanges ont eu lieu entre le CDF et les autorités impliquées dans la lutte contre la cybercriminalité au niveau cantonal et fédéral. Ces échanges ont permis au CDF de mieux comprendre au niveau global l'état de situation et les défis pour les autorités suisses liés à ce domaine de la criminalité. fedpol, le MPC ainsi que le NCSC ont pris connaissance des différentes recommandations formulées par le CDF. fedpol et le NCSC s'emploieront à leur réalisation.

Prise de position générale du MPC

Le Ministère public de la Confédération (ci-après : MPC) se détermine comme suit sur le rapport d'audit du Contrôle fédéral des finances relatif à l'efficacité de la lutte contre la cybercriminalité.

Le MPC relève tout d'abord qu'il intervient dans la mesure des considérations développées dans le rapport s'agissant des enquêtes en cours au MPC et de la collaboration avec fedpol (ch. 2.4 « Le Ministère public de la Confédération apprécie le travail de fedpol, mais des divergences subsistent ») et formule la détermination générale suivante.

Si le MPC a livré en 2017 de nombreuses procédures de phishing à fedpol, c'est qu'il a dès le printemps 2017 dédié l'activité de deux de ses procureurs et d'un procureur assistant, initialement incorporés à la division « Criminalité économique » (WIKRI), au développement de la lutte contre la cybercriminalité au niveau fédéral. L'activité de ces derniers s'est répartie entre le traitement des dossiers de phishing transmis par les ministères publics cantonaux dans la mesure où ils relevaient de la compétence fédérale, l'instruction de dossiers particulièrement complexes sur le plan technique et d'ampleur internationale, ainsi que le développement conceptuel des activités du MPC dans le domaine de la lutte contre la cybercriminalité.

En 2019, après avoir procédé à une étude stratégique, le MPC a décidé de transférer les deux procureurs et le procureurs assistant spécialisés cyber dans une nouvelle division regroupant les autres spécialistes des domaines de l'entraide, du terrorisme et du droit pénal international. Cette nouvelle division RTVC est entrée en fonction le 1er janvier 2020.

Il tient à cœur au MPC que les défis posés par la cybercriminalité soient traités de la manière la plus efficiente possible et avec les ressources les plus adéquates. A cet égard, il se réjouit de la bonne collaboration avec fedpol, collaboration qui a d'ailleurs permis de conduire rapidement une affaire devant le TPF en 2019.

De son côté, le MPC engagera tous les moyens nécessaires afin de permettre à fedpol de mener à bien les mesures prévues dans la recommandation no 5 du rapport d'audit, dans le but de dégager des conclusions susceptibles de contribuer au mieux à l'amélioration de l'efficacité de la lutte contre la cybercriminalité.

Prise de position générale du SNPC (NCSC)

Siehe konsolidierte Stn des fedpol.

1 Mission et déroulement

1.1 Contexte

Le Contrôle fédéral des finances (CDF) a agendé un examen sur l'efficacité de la lutte contre la cybercriminalité chez fedpol à son programme annuel d'audit 2019. D'une part, l'Office fédéral de la police (fedpol) soutient le Ministère public de la Confédération (MPC) et ses instructions cyber dans le cadre des compétences fédérales obligatoires et facultatives[1]. D'autre part, comme office central de police[2], fedpol apporte son aide aux cantons. Près de neuf plaintes sur dix dans le domaine de la cybercriminalité sont de compétence cantonale (infractions contre le patrimoine, intégrité sexuelle, atteinte à la réputation, pratiques déloyales, etc.). Au premier semestre 2020, environ 85 % des plaintes relèvent de la cyberescroquerie, 11 % de délits sexuels et 4 % d'atteintes à la réputation[3].

Dans son organisation, fedpol n'a pas d'unité spécifique d'enquêteurs fédéraux dédiée à la criminalité numérique, mais une division de soutien au sein de la Police judiciaire fédérale (PJF). Dénommée « IT Forensique & CyberCrime » (IFC), elle fournit ses prestations aux divisions de la PJF, au MPC et à d'autres entités fédérales ainsi qu'aux polices cantonales. L'IFC se charge aussi de la coordination avec les cantons, de la coopération internationale et du tri des dénonciations dans le domaine pédocriminel numérique[4]. La PJF dispose d'enquêteurs fédéraux avec des formations pour le domaine cyber, lesquels collaborent avec le MPC dans les procédures de cybercrminalité complexe de compétence fédérale. Ces enquêteurs sont intégrés à la division « Criminalité économique » (WK) et sont présents sur les différents sites de fedpol pour couvrir la diversité des langues nationales.

Le 18 avril 2018, le Conseil fédéral a décidé de renforcer le travail des autorités fédérales de poursuite pénale dans le cadre du volet pénal de la Stratégie nationale de protection contre les cyberrisques (SNPC II, mesures M18 à M21). Le Cyberdélégué coordonne les activités liées et surveille l'avancement de sa mise en œuvre. Il publie des rapports annuels de situation dont le dernier date d'octobre 2020. Le CDF a complété son examen par une analyse de la SNPC II, sa couverture des risques et l'avancement de sa mise en œuvre.

---

1 Dans le cadre obligatoire : le crime organisé, le blanchiment d'argent, la cybercriminalité au sens étroit (hacking, ransomware, phishing), des auteurs à l'étranger, des auteurs inconnus grâce à des techniques d'anonymisation hors du commun, un processus extraordinairement technique, plusieurs cantons et/ou Etats, etc. Pour plus de détails : MPC, *Concept sur la délimitation des compétences dans le domaine de la lutte contre la cybercriminalité*, 2018.

2 Loi fédérale sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres Etats du 7.10.1994 (LOC), RS 360 et Ordonnance sur l'exécution de tâches de police judiciaire à l'Office fédéral de la police du 30.11.2001, RS 360.1.

3 Ces chiffres proviennent de données de l'Office fédéral de la statistique (OFS) reçues durant l'audit du CDF. Une publication spécifique de l'OFS est prévue au printemps 2021.

4 Depuis le 19 décembre 2001, une convention administrative lie le Département fédéral de justice police (DFJP) à la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) sur la coordination de la lutte contre la criminalité sur Internet. Cette convention a créé le Service de coordination de la lutte contre la criminalité sur Internet (SCOCI), désormais intégré à l'IFC. Financé aux deux tiers par les cantons, le SCOCI avait un budget d'environ 1,3 million de francs. Début 2020, les cantons et le DFJP ont décidé de dénoncer la convention SCOCI. Les recherches actives en matière d'images interdites réalisées par fedpol seront stoppées fin 2020.

1.2 Objectif et questions d'audit

L'objectif de l'audit vise à examiner l'efficacité de la lutte contre la cybercriminalité chez fedpol et le volet pénal de la SNPC II, sa couverture des risques et l'avancement de sa mise en œuvre auprès du Cyberdélégué. Pour répondre à cet objectif d'audit, les questions suivantes ont été traitées :

1. fedpol est-il organisé afin de pouvoir s'acquitter efficacement de ses tâches dans la lutte contre la cybercriminalité ?
2. La coordination et la coopération entre autorités fédérales et cantonales sont-elles efficaces dans la lutte contre la cybercriminalité ?
3. Les principaux risques liés à la cybercriminalité sont-ils identifiés et traités dans la SNPC II, ainsi que dans son plan de mise en œuvre ?
4. La mise en œuvre des mesures de la SNPC II dans le domaine de la cybercriminalité est-elle appropriée ou déjà dépassée ?

Le chapitre 2 répond à la première question d'audit. La deuxième question fait l'objet du chapitre 3, alors que le chapitre 4 livre les réponses aux questions 3 et 4.

1.3 Etendue de l'audit et principe

L'audit a été mené de septembre 2019 à septembre 2020, avec des interruptions dues à la pandémie du COVID-19. Après une phase préparatoire, la phase de terrain a eu lieu de juin à septembre 2020. L'examen a été réalisé par Alexandre Bläuer (expert en audit), Hedwig Dubler (juriste), Alexandre Haederli (expert en audit, analyste de données) et Yves Steiner (responsable d'audit). Il a été conduit sous la responsabilité de Jean-Marc Stucki (responsable du Centre de compétences 2).

Une discussion des résultats de terrain avec fedpol a eu lieu le 28 septembre 2020, puis avec le Cyberdélégué le 22 octobre 2020. Ce rapport ne prend ensuite en compte que les précisions apportées par fedpol, le MPC et le Cyberdélégué dans le cadre de leurs prises de position écrites au 8 décembre 2020.

1.4 Documentation et entretiens

Les informations nécessaires ont été fournies au CDF de façon exhaustive et compétente par fedpol. Les documents requis ont été mis à la disposition de l'équipe d'audit sans restriction. Le même constat est fait s'agissant du MPC et du Cyberdélégué.

Le CDF s'est entretenu avec quatre membres de la direction de fedpol dont sa cheffe, le chef de la PJF, le chef de la division IFC à la PJF, la cheffe des ressources humaines ainsi qu'avec les collaboratrices et collaborateurs de plusieurs sections de la PJF. Des entretiens ont aussi eu lieu avec l'ancien Procureur général de la Confédération, les procureurs en charge des dossiers cyber au MPC, le Cyberdélégué de la Confédération et deux collaborateurs de l'OFS. Sous les réserves d'usage, l'OFS a livré au CDF ses futures statistiques de la cybercriminalité (publication en mars 2021) ce qui a permis au CDF d'établir un échantillon de cantons représentatif d'infractions liées à la criminalité numérique.

Le CDF a rencontré le président de la Conférence des Commandants des Polices Cantonales de Suisse (CCPCS) et le vice-président de la Conférence des procureurs suisses (CPS). Sollicités sur une base volontaire, des enquêteurs spécialisés et des cadres des polices cantonales ainsi que des procureurs des cantons d'Argovie (AG), de Bâle-Ville (BS), de Berne (BE), du Jura (JU), du Tessin (TI), de Vaud (VD) et de Zoug (ZG) ont accepté d'échanger sur le sujet ou de recevoir l'équipe du CDF. La police cantonale et le parquet du canton de Zurich (ZH) n'ont pas souhaité s'entretenir avec le CDF, alors qu'ils collaborent avec le MPC et fedpol sur des dossiers cyber d'importance nationale.

En outre, des experts en criminalité numérique et une société de prestations qui fournit des services et du matériel forensique aux autorités de poursuite pénale de la Confédération et des cantons ont été questionnés par le CDF.

1.5 Discussion finale

Une discussion finale était prévue le 3 décembre 2020. fedpol a demandé son ajournement en raison des attentats terroristes en Suisse et à l'étranger et a livré une prise de position en date du 8 décembre 2020, tout comme le MPC et le Cyberdélégué.

Une discussion finale a finalement pu être organisée en ligne le 13 janvier 2021 sur la base d'un projet de rapport adapté. Les personnes suivantes y ont participé :

- pour fedpol : la directrice, la directrice suppléante et cheffe des ressources humaines, le vice-directeur et chef de la PJF, la cheffe de la communication, le responsable des finances et du controlling, une cheffe de domaine de l'état-major de la PJF et une assistante de direction;
- pour le MPC : un procureur général adjoint et un procureur chargé des procédures de cybercrminalité complexe de compétence fédérale;
- pour le NCSC : le cyber-délégué et le coordinateur de la SNPC ;
- pour le CDF : le vice-directeur, les responsables des domaines d'examen 1 et 7, le responsable du centre de compétences 2, le responsable de révision et un expert en audit.

Le CDF remercie l'attitude coopérative et rappelle qu'il appartient aux directions d'office, respectivement aux secrétariats généraux, de surveiller la mise en œuvre des recommandations.

CONTRÔLE FÉDÉRAL DES FINANCES

2 Ressources en personnel et travail avec le Ministère public de la Confédération

2.1 Une situation contrastée dans les ressources humaines

Le personnel de la PJF dévolu aux enquêtes numériques travaille dans plusieurs entités. En taille, l'unité la plus grande est la division de soutien IFC. Elle est constituée d'une soixantaine de personnes. Outre les cadres et le personnel de soutien, 24 spécialistes forensiques IT (23,10 ETP) et 19 spécialistes police II (14,10 ETP) y sont engagés.

Les spécialistes forensiques IT ont des tâches d'investigation numérique (sauvegarde et pénétration de supports mobiles, informatiques et autres ; recherches *open source* ; analyse de crypto-monnaies, d'appareils GPS, etc.). Ils se regroupent dans les commissariats 1, 2 et 3 de l'IFC. En 2019, les commissariats 4 et 5 de l'IFC ont été fusionnés en un seul commissariat. Cette réorganisation répondait à l'évolution dans les cantons avec la création du NEDIK (voir encadré 2) et faisait suite à un départ de personnel à la PJF. Les spécialistes polices II de ce commissariat réalisent le tri d'annonces, le catalogage d'images interdites, la coordination avec les partenaires nationaux et internationaux, ainsi que des recherches actives[5].

De plus, la PJF compte une demi-douzaine d'enquêteurs qui participent à plein temps ou à temps partiel aux procédures cyber du MPC. Ils font partie de la division d'enquête contre la « Criminalité économique » (WK) et travaillent à Berne, Lausanne et Zurich. Du personnel de la division de l'Entraide judiciaire, terrorisme et droit pénal international (RTV) participe aussi à ces instructions du MPC. En outre, 258 collaborateurs de la PJF ont effectué des sessions *e-learning* Cybercrime I et II de l'Institut suisse de police (ISP). Neuf enquêteurs de la PJF ont suivi le cours de cyber-enquêteur (niveau II), cinq autres ont achevé un CAS en investigation numérique auprès des Hautes écoles spécialisées de Neuchâtel ou de Lucerne. A l'avenir, la PJF souhaite former de deux à quatre enquêteurs spécialistes en cybercriminalité par an. Au total, son réservoir d'enquêteurs susceptibles d'être formés se monte à une trentaine de personnes.

Dès 2019, fedpol a actualisé les cahiers des charges de son personnel. Le CDF constate que deux cahiers des charges existent à l'IFC (« spécialiste forensique IT » et « spécialiste police II »). Ces fonctions correspondent à la classe de salaire 24. La formulation des tâches et des objectifs définis dans ces cahiers des charges est très générique. Elle ne permet pas d'identifier les compétences et les tâches réellement effectuées par les collaborateurs de l'IFC.

L'analyse d'un échantillon représentatif de 17 dossiers n'a pas montré de lacune majeure. Les dossiers des principaux enquêteurs WK actifs sur les procédures cyber du MPC sont en adéquation avec leur fonction. A l'IFC, un dossier sur six experts forensiques apparaît peu en adéquation avec les qualifications requises pour les tâches à accomplir aux commissariats 1, 2 et 3. Chez les spécialistes police II, la situation est plus contrastée : quatre des neuf dossiers analysés n'attestent pas d'une formation de policier à l'embauche, même si des formations complémentaires en lien avec les tâches de l'IFC 4/5 ont eu lieu.

Dans l'échantillon retenu (sans tenir compte des quatre cadres), le CDF constate que 75 % des huit spécialistes police II ont atteint le niveau maximal de rémunération de la classe 24

[5] L'IFC 4/5 correspond en partie à l'ex-SCOCI, créé par les cantons et la Confédération en 2001.

en raison d'une progression selon l'ancienneté. Cette tendance est moins marquée pour les spécialistes forensique IT où deux des cinq personnes atteignent ce niveau (40 %).

Les personnes de l'IFC confrontées au contenu pornographique interdit (images pédopornographiques, zoophilie ou violentes)[6] ont l'obligation de prendre contact et de s'entretenir avec le service psychologique interne deux fois par an. En 2019, elles étaient neuf. Formellement, le CDF constate que ces contacts ont eu lieu : le processus est actif. Sur le terrain, le personnel relève que ces *debriefings* psychologiques traitent moins l'aspect « contenu » du travail que les relations avec la hiérarchie et les conditions générales de travail.

Appréciation

Sur la base des dossiers analysés, les compétences du personnel de l'IFC et de WK sont globalement en adéquation avec les tâches effectuées dans ces divisions de la PJF. C'est moins le cas des personnes de la fonction « Spécialiste police II ». La plupart d'entre elles ont toutefois suivi plusieurs cours de formation en emploi pour remplir au mieux leurs missions au sein de la PJF (langues, usage des bases de données internationales, etc.).

L'élaboration de deux cahiers des charges génériques pour le personnel de l'IFC a clarifié une situation de départ hétéroclite. Ces cahiers des charges ne donnent cependant pas une vision précise des compétences recherchées, ni un aperçu clair du personnel à recruter ou déjà recruté. La stratégie de recrutement peut s'avérer difficile. De plus, ces cahiers des charges ne reflètent pas les tâches effectives du personnel, ce qui soulève des difficultés potentielles pour évaluer ces performances lors des entretiens annuels, malgré l'existence de conventions d'objectifs individuelles.

Le système de rémunération mis en place, quant à la progression salariale selon l'ancienneté et au niveau de salaire à l'engagement a tendance à laisser peu de marge de manœuvre en l'état actuel. Pour fedpol, le salaire n'est cependant pas la motivation première à l'embauche. De son côté, le CDF observe malgré tout un risque de démotivation du personnel de l'IFC en lien avec ces paramètres, notamment chez les personnes arrivées il y a peu et/ou au bénéfice de formations plus pointues. Les employés performants risquent de voir leurs efforts insuffisamment valorisés par rapport à ceux qui sont là depuis plus longtemps. Ce risque doit être pris en compte car, sur le marché de l'emploi, plusieurs corps de police cantonaux se trouvent déjà ou vont bientôt être à la recherche d'experts, notamment dans le domaine forensique.

Recommandation 1 (Priorité 2)

Le CDF recommande à fedpol d'évaluer si la reformulation des cahiers de charges de la division « IT Forensique & CyberCrime » lui permet d'apprécier adéquatement les prestations de l'ensemble du personnel de cette division de soutien selon leur formation et leurs prestations.

Prise de position de fedpol

Das Projekt Fachliche Entwicklungsmöglichkeiten (FEM) wurde 2019 bei fedpol umgesetzt. Ziel dieses Vorhabens ist die berufliche Weiterentwicklung und die interne Mobilität der Mitarbeiter*innen zu fördern sowie die Gleichbehandlung und Entlöhnung der Mitarbeiter*innen entsprechend ihrer Aufgaben, Kompetenzen und Verantwortlichkeiten sicher zustellen. Dafür wurden die Stellenbeschriebe standardisiert und Funktionsbezeichnungen

[6] Code pénal suisse (CP), article 197 al. 4 et 5.

harmonisiert. In der Planung und Umsetzung des Projekts FEM waren das Generalsekretariat EJPD und sämtliche Direktionsbereiche fedpol vertreten. Das EPA war ebenfalls involviert und hat das Projekt und die Standardstellenbeschriebe unterstützt. Die Entwicklung des Basislohnes richtet sich nach der individuellen Leistung. Die Personalbeurteilung bildet dabei die Grundlage. Die Mitarbeitenden werden nicht nur anhand der Stellenbeschriebe, sondern den jährlich, individuell definierten Zielen beurteilt.

2.2 Le processus de création des postes en lien avec la lutte contre la cyber-pédocriminalité est peu transparent

Fin 2019, de façon inattendue, fedpol a reçu du Parlement quatre postes supplémentaires au budget 2020 pour sa lutte contre la cyber-pédocriminalité (voir annexe 4). Leur obtention se fonde sur une hausse des annonces internationales à caractère pédopornographique numérique et la nécessité de renforcer le travail d'office central de police, soit l'appui aux cantons (chapitre 3.2). Ces postes ont une dimension opérationnelle et doivent servir à la coordination nationale contre la pédocriminalité. fedpol a pourvu ces postes au premier semestre 2020.

Réalisée en quatre jours ouvrables, la répartition de ces ressources par la direction de fedpol montre que deux postes vont à la PJF, un au domaine de direction « Prévention de la criminalité et État-major de direction » et un à la communication de fedpol. Après de multiples demandes durant la phase d'audit, le CDF a été informé fin août 2020 que fedpol « *s'est penchée sur l'utilisation à bon escient des postes obtenus fin 2019* »[7]. A cette date, un email de la direction indique bien une discussion entre cadres. Cependant, aucun élément, ni document n'a pu être présenté au CDF montrant qu'une analyse des besoins a été faite pour établir cette distribution des nouvelles ressources.

Les justificatifs pour comprendre la création de ces postes (proposition de création, description du poste, cahier des charges et « décision météo »[8]) ont été livrés deux mois après la première requête du CDF. Comme l'illustre le tableau de l'annexe 5, cette création de postes montre des lacunes dans le processus des ressources humaines (documents originaux inexistants, insuffisamment complétés ou partiellement signés ; descriptions de postes partiellement remplis, pas en adéquation ou sans rapport avec la décision du Parlement ; absence de « décisions météo » dans la moitié des cas, etc.).

Au terme de l'analyse des documents et des entretiens, le CDF constate que la traçabilité de l'information entre la décision du Parlement, l'analyse de besoins réalisée par fedpol fin 2019 et la décision d'affectation des postes au premier semestre 2020 n'est pas garantie.

---

7 « Les besoins de soutien des cantons dans le domaine de la pédopornographie ayant diminué et ces besoins ayant augmenté sur un grand nombre d'autres phénomènes cyber, fedpol s'est penchée sur l'utilisation à bon escient des postes obtenus fin 2019. Pour soutenir ces trois piliers que sont la répression, la coopération et la prévention, fedpol a attribué deux postes à la PJF, un poste à la prévention de la criminalité et un poste à la communication (…). La criminalité digitale ne peut pas seulement être combattue avec des moyens répressifs. En accord avec sa stratégie et les besoins identifiés, un poste a été confié à la prévention afin d'assurer la collaboration avec les autorités fédérales, cantonales et les NGO. Enfin la sensibilisation de la population en Suisse est importante, fedpol répond à de nombreuses questions médiatiques sur le sujet et effectue également la coordination nationale et internationale avec les cantons et les organisations internationales comme Europol. C'est pourquoi le quatrième poste a été attribué à la communication » (fedpol au CDF, email, 21 août 2020).

8 Du nom de la décision qui valide formellement l'ouverture du poste au concours chez fedpol.

Appréciation

Le processus de création des postes supplémentaires acceptés par le Parlement comporte des manquements. A la fin de l'audit, la documentation reçue pour chacun de ces postes était lacunaire. Il subsiste encore un doute sur un document réalisé pour répondre aux requêtes du CDF. Le processus dit « décision météo » qui valide la création de postes chez fepdol n'est pas suffisant : proposition de création non-signée, ouverture de postes non-documentée via les « séances météo », décision directoriale d'embauche remplacée par une liste Excel… Pour le CDF, la gestion de ce processus et de la documentation par le service des ressources humaines n'est pas transparente.

Le CDF émet des doutes sur l'allocation des postes décidée par fedpol. Fin 2019, le Parlement a exprimé sa volonté de lutter contre la cyber-pédocriminalité, d'ancrer ces nouveaux postes dans l'opérationnel et en appui aux cantons. Lors des entretiens, plusieurs interlocuteurs – fédéraux et cantonaux – ont aussi insisté sur les besoins en termes de coordination, de traitement de l'information et d'analyse dans le domaine cyber (point 3.1).

En suivant l'intention formulée de la proposition Meyer adoptée par le Parlement (voir annexe 4), le CDF estime que les nouveaux postes attribués à fedpol devaient être alloués à la PFJ et à ses divisions Analyse criminelle (AC) et IFC. Depuis 2018, la division AC produit un rapport pour les cantons sur la pédocriminalité. Le processus d'assurance-qualité des données issues des partenaires cantonaux lors de l'élaboration de ce rapport est perfectible. Pour le CDF, la création d'un poste dans la division AC répond bien à ce besoin d'améliorer la qualité de ce rapport et l'analyse dans le domaine de la pédocriminalité. Par ailleurs, la création d'un poste de conseiller spécialisé à l'Etat-major de la PJF correspond à des besoins de coordination que le CDF a aussi identifié et peut comprendre.

En revanche, le CDF ne comprend pas pourquoi le commissariat IFC 4/5 ne reçoit pas de poste. Ce commissariat – doté d'une vingtaine de personnes avec près d'un millier d'heures supplémentaires sur la période 2018–2020 – réalise notamment le travail de tri, de catégorisation, d'analyse et de suivi des annonces venues de l'étranger (NCMEC, CLEMONA, Europol, Interpol, etc.). Ces tâches coïncident avec les vœux du Parlement. Une analyse des besoins documentée par fedpol aurait permis de justifier son choix.

Les deux derniers postes – pour des campagnes de préventions et un porte-parole à la communication – n'ont pas de lien étroit avec la décision du Parlement. Ces postes présentent des manques formels importants dans la documentation des ressources humaines.

Ainsi, fedpol n'a pas totalement respecté la décision du Parlement de créer des nouveaux postes de travail liés à la lutte contre la pédocriminalité. Les explications livrées a posteriori ne remplacent pas une documentation claire et une analyse circonstanciée des besoins.

Recommandation 2 (Priorité 1)

Le CDF recommande à fedpol de réexaminer l'allocation des ressources supplémentaires accordées par le Parlement pour la Police judicaire fédérale. Cette analyse doit lui permettre d'apporter la preuve du renforcement de la lutte contre la cyber-pédocriminalité et d'en démontrer la plus-value.

Prise de position de fedpol

Die vom Parlament gesprochenen Stellen zur Verstärkung der Bekämpfung der Pädokriminalität wurden nach interner Analyse dort eingesetzt, wo sie die grösste Wirkung erzielen

können. Fedpol überprüft den Einsatz, die Effizienz und Effektivität der eingesetzten Stellen laufend und passt die Allokation der Stellen bei Bedarf an.

2.3 L'environnement informatique et les outils de pilotage de la Police judiciaire fédérale sont à améliorer

Environnement numérique et traitement des données d'enquête

Déjà lors de la préparation d'audit, le CDF a constaté des difficultés liées à l'environnement informatique de la PJF. La direction de fedpol a eu connaissance en janvier 2019 de plusieurs faiblesses qui compliquent le travail de la PJF. Les entretiens du CDF auprès des cadres et du personnel de la PJF ont confirmé les constats suivants lors de l'audit :

- Le personnel de la PJF travaille avec un environnement informatique de huit applications ou supports[9] pour le traitement des données d'enquête et le suivi des dossiers transmis par des autorités dont le MPC et les autorités de poursuite des cantons.
- Cet environnement complexe provoque notamment des doubles à quadruples saisies dans plusieurs applications et des pratiques d'archivages individualisés de documents d'enquête. Il y a aussi une absence d'interopérabilité entre applications, ou encore, des transferts et des reconstitutions d'informations laborieuses.
- Cette situation ne permet pas de limiter le risque d'erreurs inhérentes à des manipulations manuelles (copier-coller, bases Excel, absence d'historiques et logs, traçabilité automatique impossible, etc.). Elle ne permet pas non plus d'éviter la production de documents – rapports de police, procès-verbaux d'auditions, analyses, etc. – à de multiples exemplaires, comportant le risque de ne pas toujours pouvoir juger des différences en raison de l'absence de traçabilité.

Malgré des mesures de circonstances prises dès janvier 2019, la PJF admet une perte d'efficacité et d'efficience dans le suivi des dossiers d'enquête et le traitement des données numériques. Le chef de la PJF note un besoin prépondérant pour améliorer les conditions de travail de son personnel. Selon la direction de fedpol, ce point fait partie du programme « Ermittlungssystem » (ErmSys) qui doit permettre de résoudre ces problèmes. Le calendrier communiqué au CDF par fedpol prévoit l'aboutissement de ce projet fin 2022.

Appréciation

La réalité du traitement numérique des données d'enquête à la PJF porte des risques évidents pour la qualité du travail des enquêteurs fédéraux à l'égard de ses partenaires. La direction de fedpol doit garantir un environnement de travail adéquat, sûr et avec toutes les assurances de traçabilité des analyses réalisées qui doivent être dûment documentées.

La situation actuelle répond en partie à ces objectifs. Décrite en janvier 2019 par le chef de la PJF à sa direction, le CDF estime que cette dernière aurait dû prendre des mesures urgentes et prioritaires. L'échéance fixée à 2022 pour combler les lacunes constatées est optimiste. Cela nécessite une concentration des ressources pour atteindre l'objectif fixé et l'amélioration des conditions de travail, comme l'efficience du travail des collaborateurs.

Ces points sont intégrés dans la recommandation 3 de ce rapport.

[9] Il s'agit d'OPGKBKP, Outlook, Excel (Falllist Frontrapport), PT/CATS, ORMA, ISS, Janus, FAP et du serveur P.

Outils de pilotage à disposition de la PJF

Le CDF a noté des manques dans l'usage quotidien des outils de gestion des affaires par le personnel de la PJF. Après une analyse de données, le CDF n'a pas pu quantifier clairement les prestations de fedpol aux cantons, tant à partir du suivi des dossiers (application ORMA) qu'avec la gestion des heures de travail (PT/CATS). Sous ORMA, les règles de saisies ne sont pas clairement suivies par le personnel de la PJF. La catégorisation des affaires selon des phénomènes liés à la cybercriminalité est irréalisable. Pour les heures de travail (PT/CATS), les règles de saisie ne sont pas assez précises pour chiffrer le volume des heures réalisées pour les cantons. Une catégorie « fourre-tout » *(catch-all)* pour les prestations aux cantons empêche une répartition transparente des activités pour leur bénéficiaire.

Le CDF n'est ainsi pas parvenu à désenchevêtrer les prestations aux cantons sous le régime de la convention SCOCI (et financées aux deux tiers par tous les cantons). Elles sont livrées individuellement aux cantons et réalisées dans le cadre de l'échange de bons procédés[10].

La PJF n'a pas d'indicateurs immédiats de suivi (nombre d'enquêtes ou de requêtes en cours, en suspens ou bouclées ; taux de requêtes et d'échecs selon le type de prestations ; taux de performance des outils forensiques, définition et mise en place d'indicateurs de type *redflags*…). Pour les annonces internationales d'images interdites, l'IFC ne fait pas de suivi systématique des dénonciations aux cantons bien que des outils légaux[11] existent pour le faire sans contraindre ses partenaires cantonaux (chapitre 3.2). Des indicateurs peuvent néanmoins être créés *a posteriori*, mais au prix d'un effort important de consolidation. Il n'est donc pas possible de créer des indicateurs objectifs pour juger de l'efficacité des prestations de la PJF à l'égard de ses partenaires, notamment dans la criminalité sur Internet.

Des mesures correctives ont toutefois été prises. D'une part, la PJF a entrepris courant 2019 la modification et l'adadptation des catégories dans PT/CATS. Dès le 1er janvier 2021, cette optimisation devrait être en place, notamment afin de pouvoir identifier les prestations livrées par la PJF aux cantons. D'autre part, le chef de la PJF a instauré le 1er janvier 2019 une réunion bilatérale avec le chef de la division IFC pour améliorer l'aspect suivi. Il juge aussi que la mise en place d'un système de monitoring de type tableau de bord *(cockpit)* pour les activités de la PJF serait profitable. Démarré début 2020, le projet « PlaVis » du domaine « Gestion des ressources et stratégie » a comme but de produire une visualisation d'indicateurs clé pour la direction de fedpol d'ici 2022. Ce projet ne comporte toutefois pas de dimension spécifique aux besoins de la PJF.

Appréciation

L'absence d'instruments performants et automatisés de pilotage des activités de l'IFC et, plus généralement de la PJF, pose des défis à la gestion opérationnelle. Cette absence génère le risque d'une conduite peu factuelle, sans suivi clair des dossiers en cours et limitée dans sa capacité à anticiper des problèmes futurs. L'exemple du traitement inefficient de plus de 170 dossiers de *phishing* (chapitre 2.4) illustre ces difficultés opérationnelles très concrètes rencontrées par l'état-major de la PJF. Dans un autre domaine, le suivi des dénonciations issues des annonces internationales en matière d'images interdites transmises

10 Ce manque de transparence n'a jamais fait l'objet de demandes d'explication des cantons ou de la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) auprès de fedpol.

11 Ordonnance sur l'exécution de tâches de police judiciaire à l'Office fédéral de la police, article 3, al. 2. let a et b et article 4 al. 1 let a.

aux cantons doit faire partie de ce monitoring et la récolte des données pour ce suivi doit également faire l'objet d'une assurance-qualité de la part de la PJF (chapitre 3.2).

Pour le CDF, il convient à chaque office de clarifier les tâches à effectuer par son personnel et à s'assurer que celles-ci sont reportées correctement dans l'outil de gestion des heures de travail (PT/CATS). fedpol ne peut pas œuvrer avec des centaines de catégories de temps de travail ce qui met son personnel dans une position difficile au moment de reporter son temps de travail effectivement réalisé dans l'outil à disposition.

Depuis 2017 dans le Compte de la Confédération, fedpol a comme seul objectif dans la lutte contre la criminalité sur Internet : « les autorités de poursuite pénale suisses et étrangères sont soutenues efficacement »[12]. L'unique indicateur retenu – le nombre de dossiers transmis aux ministères publics suisses pour des infractions poursuivies d'offices – n'est pas suffisant pour confirmer ou pour infirmer la réalisation de l'objectif défini. De nouveaux indicateurs devraient être développés afin de livrer une appréciation mieux fondée de cet objectif.

Recommandation 3 (Priorité 1)

Le CDF recommande à fedpol de rendre prioritaire le projet « ErmSys » et sa composante propre à améliorer le traitement des données à la Police judiciaire fédérale (PJF) et ce, afin de garantir un cadre de travail adéquat, efficient et efficace au personnel et aux divisions de la PJF.

Prise de position de fedpol

fedpol accepte la recommandation telle que formulée par le CDF.

Recommandation 4 (Priorité 1)

Le CDF recommande à fedpol de renforcer le pilotage des activités de la Police judiciaire fédérale par l'élaboration d'un monitoring avec un cockpit et des indicateurs pertinents pour garantir le suivi de ses dossiers. Ce monitoring devrait intégrer un suivi des dénonciations issues des annonces internationales en matière d'images interdites auprès des cantons, avec un processus d'assurance-qualité des données obtenues de ces derniers.

Prise de position de fedpol

fedpol accepte la recommandation telle que formulée par le CDF.

2.4 Le Ministère public de la Confédération apprécie le travail de fedpol, mais des divergences subsistent

Les divisions IFC et WK de fedpol contribuent aux procédures du MPC. Celui-ci a créé fin 2019 une équipe dédiée à la cybercriminalité dans sa division désormais renommée « Entraide judiciaire, Terrorisme, Droit pénal international, Cyber » (RTVC). Les réflexions sur ce changement organisationnel avaient débuté à l'été 2019. L'équipe cyber du MPC se compose de deux procureurs (arrivés de la division « Criminalité économique »), d'un procureur assistant et d'un stagiaire. Ces cyberprocureurs animent aussi les réunions ponctuelles du Cybercase, une structure d'échanges d'informations et de coordination au niveau des procureurs suisses. A l'été 2020, cette sous-division instruisait quelque 110 procédures dont la

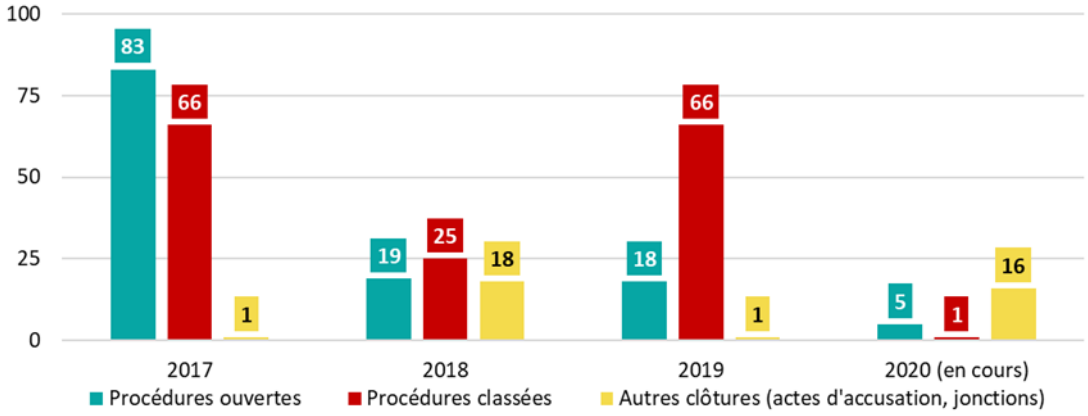
[12] Compte d'Etat, tome 2, édition 2019, p. 227.

quasi-majorité est liée à la reprise de cas cantonaux de *phishing*[13]. Ces cas d'hameçonnage de données expliquent les grands nombres des statistiques du MPC (graphique 1).

La cybercriminalité complexe occupe désormais à elle seule cinq procédures[14]. Une affaire a été classée en 2020, l'auteur ne pouvant pas être identifié. Jusqu'ici, le MPC a mené deux procédures à terme devant le TPF en 2019 : la première a été un succès, la seconde n'a pas totalement porté ses fruits (encadré 1). Ces cas montrent les défis posés par la dimension internationale de la cybercriminalité pour les autorités suisses. Pour les cyberprocureurs, il y a des difficultés liées à la lourdeur administrative dans le cadre de l'entraide internationale en matière pénale (EIMP)[15] et d'autres à la compréhension du TPF en matière cyber.

MPC - Procédures pénales en lien avec la cybercriminalité (2017 - 2020, en cours)

Ces chiffres comprennent le cas de reprise des cantons (affaires dites de *phishing*)



Remarque : ces chiffres livrés par le MPC sont des approximations, consolidées a posteriori. Ce dernier n'a pas d'instrument statistique lui permettant encore de distinguer les cas de cybercriminalité des autres enquêtes

Graphique 1 – Ouvertures, classements et autres clôtures d'instructions pénales fédérales (source : MPC).

Lors des entretiens avec la direction du MPC et les cyberprocureurs, ceux-ci ont jugé globalement positif le soutien livré par fedpol aux instructions en cybercriminalité complexe, tout comme la qualité de ses prestations forensiques et la coordination internationale.

Dès 2017, le MPC a livré à la PJF des cas de *phishing* repris à l'origine de procédures cantonales. Il voulait savoir si des modes opératoires communs existaient entre eux. L'analyse d'environ 170 dossiers a engendré des difficultés de traitement à la PJF. Celle-ci a mis sur pied le 3 juillet 2020 un groupe de travail entre les divisions IFC et WK pour éliminer une septantaine de cas en suspens (« opération truite »). La PJF reconnaît un manque d'efficacité et d'organisation du travail d'analyse. A l'époque, elle n'avait pas d'outils d'analyse performants (détection de séries criminelles). Cette situation a évolué avec l'emploi de la base de données PICSEL (projet pilote) et l'introduction des affaires de *phishing* dans cette base (encadré 4). Des premières séries auraient été identifiées. Selon fedpol, le travail

13 Depuis 2011, le Tribunal pénal fédéral (TPF) a jugé le MPC compétent pour les situations dans lesquelles les auteurs ont agi à l'étranger. Les criminels qui passent à l'acte depuis la Suisse sont poursuivis par les autorités pénales cantonales. Entre 2012 et 2017, près de 400 procédures pénales pour hameçonnage de données avaient été classées par le MPC (lire à ce propos *NZZ am Sonntag*, 28 mai 2017).

14 Il s'agit des procédures pénales de compétence fédérale (Cyber II, Massada, Zigor, Dark Silent et Truite) qui occupent cinq enquêteurs principaux de la division WK, épaulés par huit autres enquêteurs de la PJF selon les missions.

15 Le CDF a déjà constaté cela au point 5.4 de son évaluation sur l'EIMP (PA 18293), disponible sur son site Internet.

d'analyse a été finalisé fin octobre 2020. De son côté, le MPC attend encore le retour d'une centaine de dossiers de la PJF. Jusqu'ici, malgré leur traitement par fedpol, ces cas de *phishing* ont été classés par le MPC en raison de l'obsolescence des faits.

Les visions du MPC et de fedpol divergent sur la création d'une équipe d'enquêteurs dédiés à la seule cybercriminalité à la PJF. Pour plus d'efficacité, ces entités présentent des similitudes structurelles sur leur organigramme (« effet miroir »). Le MPC désire que sa division RTVC trouve son homologue à la PJF[16]. En effet, la division de l'Entraide judiciaire, terrorisme et droit pénal international (RTV) de la PJF n'a pas de sous-division Cyber. Les cyberprocureurs craignent que l'expérience des enquêteurs de la PJF – notamment avec deux personnes en particulier – ne soit pas entièrement mise à profit dans le cadre de futures procédures pénales, en raison d'un choix inapproprié au niveau des ressources de la PJF.

La direction de fedpol ne partage pas la vision du MPC. Elle l'assimile à une conception désuète de la façon d'appréhender la cybercriminalité. Du côté de la PJF, le changement survenu avec la création de RTVC a surpris. Elle comprend les besoins du MPC et reconnaît la nécessité d'avoir davantage d'enquêteurs avec des compétences cyber. Elle aborde la question sous l'angle de la transversalité, des réseaux internes de collaboration et veut rester flexible dans l'allocation des ressources. Par le passé, l'attribution d'enquêteurs au seul blanchiment d'argent avait engendré une utilisation sous-optimale des ressources. La création d'un « cyber-commissariat » ou d'une équipe multidisciplinaire n'entre pas dans la vision de fedpol. Mi-septembre 2020, fedpol et le MPC se sont réunis pour évoquer ces divergences de points de vue sans trouver de solution définitive.

Appréciation

La PJF a dû analyser un grand volume de dossiers de *phishing*. Un délai de trois ans pour cette mission relève un manque d'efficacité. Le CDF y voit aussi un manque d'outils de pilotage et de suivi des dossiers livrés par le MPC à la PJF (chapitre 2.3 et recommandation 4). Pour des questions de priorité, le MPC a focalisé son énergie sur les affaires de cybercriminalité complexe. Durant ces trois ans, il a eu toutefois des contacts avec la PJF pour connaître l'avancée de ces « petites affaires » liées au phishing. Au CDF, la PJF a encore expliqué qu'entre juillet et août 2020, l'analyse des cas de *phishing* avait livré des résultats prometteurs. Si c'est le cas, la PJF doit s'assurer que tous les cas livrés par le MPC sont désormais intégrés dans la base de données PICSEL et ainsi augmenter les chances d'identifier des séries criminelles à l'avenir.

Le CDF note la surprise de la PJF suite au changement organisationnel du MPC, alors que les travaux chez ce dernier avaient démarré six mois avant le changement effectif. Ceci traduit une communication insuffisante entre les deux entités sur un point fondamental de leur coopération. Point fort de cette coopération, « l'effet miroir » recherché entre les deux organigrammes est au cœur de la réorganisation des deux entités depuis cinq ans. Cette perte de « l'effet miroir » et ce défaut de communication nuisent à l'efficacité de la lutte contre la cybercriminalité. Dans l'intervalle, fedpol doit garantir la mise à disposition des ressources nécessaires et compétentes pour les procédures pénales « cyber » du MPC.

[16] MPC, *Massnahmenempfehlungen Cyberkriminalität bis 2023 – Validiert durch GL am 29. April 2019* (Nr. 2) MPC, *Umsetzungsplan – Cybercrime* (Nr. 2.1 & 2.2), juin 2020.

Recommandation 5 (Priorité 1)

D'ici juillet 2021, le CDF recommande à fedpol de faire une analyse des avantages et des inconvénients liée à un changement de son organisation avec la création d'un cyber-commissariat dans la division de l'Entraide judiciaire, terrorisme et droit pénal international, ainsi que d'évaluer avec le Ministère public de la Confédération, le type d'organisation permettant de garantir la gestion efficiente des enquêtes que ce dernier lui confie.

Prise de position des audités

fedpol accepte la recommandation telle que formulée par le CDF.

Encadré 1 – Un demi-échec et un succès devant les juges du Tribunal pénal fédéral

Avant la création de l'unité spécialisée cyber du MPC, ce dernier a mené un dossier jusqu'au TPF. Basés en Thaïlande, trois hackeurs s'étaient emparés de données de plus de 180 000 cartes de crédits appartenant à des personnes dans 150 pays du globe dont la Suisse. Une fois identifiés, ces informaticiens ont été arrêtés et incarcérés à Berne. Les prévenus ont avoué, collaboré à l'enquête et accepté une procédure simplifiée et trois ans de prison. Soumis au TPF, ce dernier a estimé en octobre 2016 que le MPC ne pouvait poursuivre les prévenus que sur les vols commis contre des personnes résidantes en Suisse. Dans l'ordonnance pénale rendue par le MPC en janvier 2019, les prévenus écopent d'une peine de six mois de prison sur la partie helvétique des délits (942 cartes) et des dédommagements pour les journées excessives de préventive. Les frais de procédure ont dépassé les 700 000 francs et plus de 130 000 francs de dédommagements.

Dans un autre dossier, le MPC a ouvert début 2017 une instruction contre X pour soupçons d'utilisation frauduleuse par métier d'un ordinateur[17]. En lien avec un réseau international, une personne soutirait des données de e-banking via des appels téléphoniques *(Voice Phishing)*. Au total, 2,2 millions de francs ont été transférés. En Suisse, plus de 130 plaintes ont été déposées dont une septantaine de personnes privées. L'instruction du MPC a été confrontée aux lourdeurs de l'EIMP, avant d'être facilitée par la collaboration d'une grande banque du pays. L'un de ces enquêteurs internes a accepté d'être placé sous surveillance téléphonique durant deux mois et de devenir une victime potentielle du criminel. Avec cette surveillance téléphonique et l'aide de la police hollandaise, de fedpol et d'Eurojust, il a été possible d'identifier une femme située à Rotterdam, de l'arrêter et de l'emprisonner fin juillet 2018. La prévenue a accepté une procédure simplifiée[18]. L'acte d'accusation du MPC déposé en mars 2019 demandait 30 mois de prison, dont 20 avec sursis et le règlement des frais de procédure (environ 80 000 francs). Le TPF a suivi le MPC.

17 Code pénal suisse, article 147 al. 1 en relation avec l'al. 2.
18 Code de procédure simplifiée, art. 358ss. Voir glossaire.

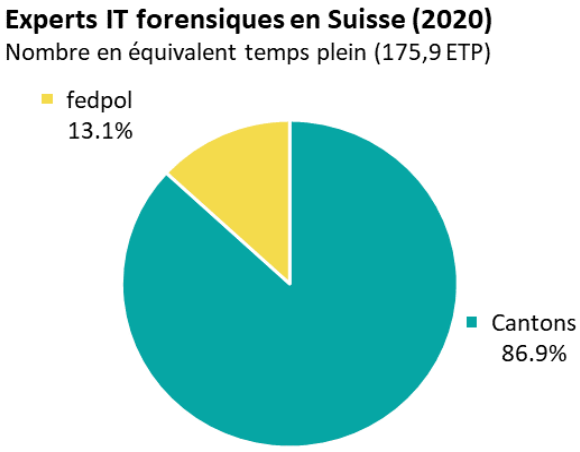
3 fedpol soutient le travail des cantons

3.1 Les cantons saluent l'essentiel de l'aide apportée par fedpol

La Loi fédérale sur les Offices centraux de police criminelle (LOC) prévoit que la Confédération dirige des offices centraux contre le crime international organisé et le trafic illicite des stupéfiants. Cette loi décrit, entre autres, leurs tâches, la nature de leur collaboration avec les autorités cantonales, étrangères et avec les offices fédéraux, ainsi que les principes du traitement des données personnelles. De plus, la coordination du travail de police transfrontalier relève de la compétence de fedpol en sa qualité d'office central de police judiciaire. Cet office assume des tâches de coordination et d'investigation préliminaire dans le but d'empêcher et de poursuivre les infractions indépendamment de savoir si l'affaire relève après de la compétence fédérale, cantonale ou d'un Etat étranger[19].

L'ordonnance sur l'exécution de tâches de police judiciaire définit les missions de la PJF[20]. Cette dernière assure « le contact avec les autorités de poursuite pénale et de police suisses et étrangères » et le « bon déroulement des enquêtes tant sur le plan des délais que sur le plan technique » dans le cadre de ses activités de coordination[21]. Le cadre légal ne définit pas d'office central de lutte contre la cybercriminalité[22]. C'est un des buts de la SNPC II (mesure M21). D'ici fin 2022, fedpol et l'Office fédéral de la justice (OFJ) mènent le travail pour réviser et adopter une modification de la LOC afin de créer un office central de lutte contre la cybercriminalité et les bases légales pour la collaboration avec les cantons.

Acceptée par le Parlement, la Loi fédérale sur les mesures policières de lutte contre le terrorisme (MPT) crée cet office central de lutte contre la cybercriminalité[23]. Cette loi est contestée par voie de référendum, avec un délai référendaire au 14 janvier 2021.



Graphique 2 – Experts IT forensiques (source : CCPCS, 9/2020)

Dans ce contexte, la PJF soutient les cantons dans le domaine forensique IT, de la coopération internationale ainsi que dans la lutte contre la cyber-pédopornographie (lire plus bas). Dans les entretiens, les cantons consultés jugent que la qualité des prestations forensiques des commissariats IFC 1, 2 et 3 est bonne. Le contenu du travail et des résultats ne souffre d'aucune critique majeure. Les délais sont en principe tenus par la PJF. Celle-ci a une infrastructure que peu de cantons ont, voire pas du tout. Ses 23,1 ETP en ressources forensiques IT constituent 13,1 % du total national (graphique 2). Il existe d'importantes variations entre des cantons dépourvus de spécialistes et d'autres avec des unités dédiées. Les cantons visités par le

19 LOC, article 2 et Code de procédure pénale, CPP (RS 312.0), article 27, al. 2.
20 Ordonnance sur l'exécution de tâches de police judiciaire à l'Office fédéral de la police du 30.11.2001.
21 Ibid., article 3, al. 2 a et b.
22 L'ordonnance indique qu'en tant qu'office central, la PJF lutte contre le crime organisé, le trafic illicite de stupéfiants, la fausse monnaie, la traite des blanches et la circulation des publications obscènes.
23 MPT du 25.9.2020, article 2a, al. f et message du Conseil fédéral concernant la MPT, FF 2019, p. 4611-4612.

CDF et la CCPCS saluent la qualité de l'échange d'informations pratiques avec l'IFC 4/5 et l'aide que celui-ci fournit pour la coopération policière internationale. Selon la CCPCS, fedpol devrait avoir plus de forces dans ce volet international pour couvrir les besoins des cantons qui mènent des enquêtes vers l'étranger. Du côté de fedpol, ce besoin devrait être pris en considération dès lors que l'IFC 4/5 cessera d'effectuer la saisie des données dans la base PICSEL en faveur des cantons qui n'ont pas les ressources pour effectuer cette opération. Cette aide est vue comme provisoire par fedpol et il attend des cantons qu'ils prennent leurs responsabilités dans le futur travail de saisie de données dans la base PICSEL.

Sur le terrain, le CDF a constaté que l'analyse des phénomènes liés à la cybercriminalité est inexistante dans les polices cantonales, en raison d'un manque de ressources dans le domaine des policiers spécialisés dans l'analyse cyber. Chaque mois, ces corps de police ont un accès privilégié aux premières statistiques de l'OFS sur la cybercriminalité (dont la publication interviendra au printemps 2021). Ils n'utilisent pas ces données à des fins d'analyse pour orienter la définition de leur propre stratégie, ou leur travail opérationnel ou de prévention. Pour ces polices, fedpol devrait faire ce travail d'analyse des phénomènes liés à la cybercriminalité. Cette tâche ne devrait pas être réalisée par le réseau NEDIK, en cours d'élaboration (encadré 2). Selon fedpol, la clarification des rôles reste à déterminer une fois la phase d'évaluation de la base de données PICSEL achevée.

Encadré 2 – Un réseau national de soutien aux enquêtes cyber en construction

Le « Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung » (NEDIK) a été créé le 14 mai 2018. En août 2020, ce groupe de travail de la CCPCS regroupait douze membres des différents concordats de police et fedpol. Son directeur devait assurer la création d'une vue d'ensemble des phénomènes de cybercriminalité ; coordonner l'essor et l'émulation de nouvelles méthodes et l'échange d'expériences ; s'assurer de la diffusion d'informations dans les petits corps de police *(best practices)* ; encourager la collaboration intercantonale dans les cyber-investigations ; définir des contrats de prestations et les prestations en elles-mêmes entre les centres régionaux ; et établir un catalogue de prestations et des produits offerts par les centres de compétences aux corps de police.

Plusieurs de ces tâches recoupent des objectifs fixés dans les mesures de la SNPC II (chapitre 4.1). C'est le cas de la création de la base de données PICSEL (vue d'ensemble des phénomènes – M18) et des bases légales pour la collaboration et la facturation des prestations entre Confédération et cantons, ainsi qu'entre cantons eux-mêmes – M19).

Pour les experts, ce réseau de spécialistes établit un échange d'informations opérationnelles. Au terme de l'audit sur place, le statut et le lien de subordination du NEDIK restaient à clarifier, comme son financement. Juridiquement, des bases légales pour l'échange d'informations entre polices faisaient encore défaut dans plusieurs cantons. L'objectif d'un catalogue national de prestations n'était pas atteint. Des règles claires sur l'usage et le financement de ces prestations manquaient encore. Pour les acteurs de terrain, la création du NEDIK est compliquée en raison des barrières fédéralistes et d'un manque de décisions politiques claires.

Selon une convention entre le CCDJP et la CCPCS acceptée le 12 novembre 2020, l'organisation et le financement des prestations du NEDIK sont désormais régies et entreront en force dès le 1er janvier 2021[24]. Le CDF n'a pas eu accès à cette convention administrative, signée lors de la phase de rédaction du présent rapport d'audit.

[24] CCDJP, *Renforcement des efforts cantonaux contre la cybercriminalité et la pédocriminalité*, 17 novembre 2020.

Appréciation

Bénéficiaires des prestations de la PJF, les cantons apprécient son travail forensique IT, ainsi que ses activités de coordination et d'échange d'informations pratiques. La PJF remplit de la sorte une partie essentielle de sa mission d'office central de police. Avec les cantons, le CDF estime qu'en terme de vue d'ensemble des phénomènes liés à la cybercriminalité, la PJF est la mieux placée pour élaborer une analyse de ces phénomènes et des tendances de la criminalité numérique. Tous les cantons visités pointent les besoins en la matière et regrettent de ne pas pouvoir le faire, faute de ressources à moyen terme. Le NEDIK est pour eux un outil d'abord opérationnel, propre à réagir dans le cadre d'enquêtes, et indisponible pour l'analyse.

Pour le CDF, la PJF doit consolider ses capacités d'analyse de la cybercriminalité. Elle a un accès aux statistiques de l'OFS en la matière et à la base de données PICSEL (encadré 4). Comme point de contact international, fedpol dispose aussi d'une vision des tendances hors de Suisse. Comme écrit dans la recommandation 2, il conviendrait d'examiner une réallocation des postes du Parlement pour renforcer les capacités d'analyse.

3.2 Clarifications bienvenues contre la cyber-pédopornographie

La poursuite pénale de la pédocriminalité est une tâche cantonale. En grande majorité, les infractions en ligne ont un lien avec l'étranger[25]. Selon la LOC, fedpol assume un rôle d'office central dans cette lutte et assure une interface entre l'étranger, elle-même et les polices cantonales. Comme Centre de compétences national en matière de cybercriminalité (NC3), fedpol assure l'échange d'informations avec Interpol et Europol, l'exploitation du point de contact unique 24h/24 (Convention sur la cybercriminalité de Budapest – CCC) et le travail avec le National Center for Missing and Exploited Children (NCMEC). Jusqu'à fin 2020, fedpol réalise aussi des recherches actives. Tout ce travail de tri et de recherche a donné lieu en 2019 à la livraison de plus de 1500 dénonciations aux cantons.

Annonces internationales (Interpol, Europol, CCC, NCMEC)

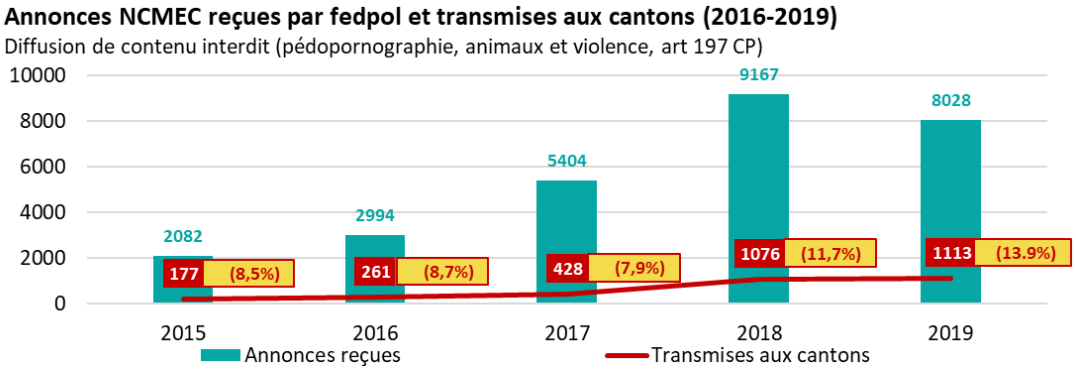
La majorité des cas remis aux cantons provient du réseau NCMEC. En 2019, l'IFC 4/5 a trié 8028 annonces de ce type avec des images interdites – pédopornographiques, zoophiles ou violentes. Il a livré 1113 dossiers aux cantons. Dans ces cas, le criminel présumé est identifié par fedpol et le contenu répréhensible est conservé comme preuves. Entre 2015 et 2019, ce commissariat élague en moyenne neuf dossiers sur dix (graphique 3). La part de cas remis aux cantons s'accroît pourtant rapidement : de 8,5 % en 2015 à 11,9 % en 2019. En volume, quatre cantons (ZH, AG, BE et VD) ont reçu la moitié des dossiers (559 sur 1113).

Pour les cantons, ce flux continu de dossiers NCMEC et son essor rapide sont un défi. Une analyse de fedpol en juin 2019 indique que, pour 18 corps de police, ceux-ci n'ont pas été proactifs dans le traitement des annonces NCMEC jusqu'à fin 2017, d'où une hausse des dossiers en suspens[26]. En juin 2019, ces mêmes polices n'ont pas ou n'allouaient pas plus de 15 % en moyenne de leurs postes à la lutte contre la criminalité pédosexuelle en ligne.

[25] Car les criminels agissent depuis l'étranger, ou les victimes ne se trouvent pas en Suisse et à l'étranger, ou bien les moyens ayant servi à commettre l'infraction et les preuves proviennent de fournisseurs d'accès étrangers.

[26] *Pädosexuelle Kriminalität im virtuellen Raum*, juin 2019, p. 25.

Dans ses entretiens, le CDF observe que pour quatre cantons visités sur cinq, les ressources du ministère public et/ou de la police cantonale manquent drastiquement pour traiter le flux d'annonces livrées par fedpol. Parfois, les cas en suspens vont jusqu'à un an et des choix dans la réponse pénale donnée à ces dossiers sont contestés (encadré 3).



Graphique 3 – Tri des annonces NCMEC par fedpol et livraison des cas pénalement pertinents aux cantons (source : fedpol).

Pour les cantons visités, la qualité des dossiers reçus de fedpol est assez bonne. Des policiers et des procureurs cantonaux jugent cependant que le triage pourrait être amélioré, notamment si un cas NCMEC inclut une seule image prohibée. Pour fedpol, en application du droit pénal, si l'image en question revêt un caractère d'infraction, la transmission aux autorités de poursuite pénale cantonales est indiscutable. Enfin, pour un canton, il serait utile d'éviter de bloquer automatiquement le profil de la personne qui a partagé un fichier illégal sur un réseau social et ce, afin d'obtenir plus vite des données utiles à son identification.

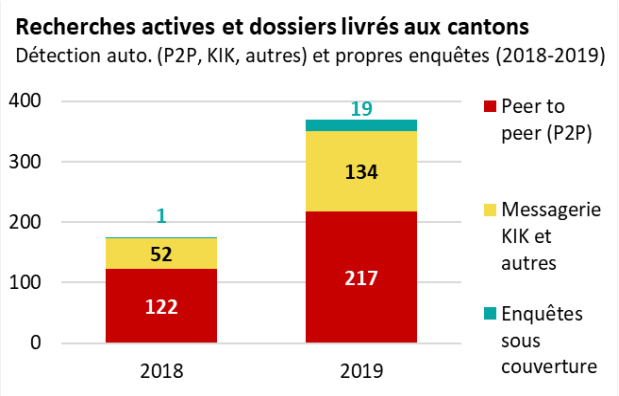
Encadré 3 – Pratiques de circonstance pour éviter l'engorgement dans les cantons

En 2019, un canton a reçu plus de 130 annonces NCMEC, une vingtaine d'annonces issues de recherches actives (fedpol) et trois annonces d'Europol. Les cas NCMEC submergent les policiers en charge de la cyber-pédocriminalité dont les ressources se montent à 1,6 personne (ETP). Pour éviter l'engorgement, le parquet et la police du canton ont convenu d'envoyer des lettres d'avertissement aux personnes concernées si les images relèvent de la zoophilie et, pour la pédopornographie, si l'affaire est une première, relève de l'indignation ou de la plaisanterie. En 2019, près de 90 % des annonces NCMEC n'avaient pas été traitées à la date de l'entretien avec le CDF. La police d'un autre canton envoie les cas NCMEC directement au parquet. Celui-ci ouvre une instruction puis la classe. Si un second cas NCMEC sur la même personne arrive de fedpol, le parquet ouvre alors une nouvelle procédure et instruit avec plus de conviction.

Ces pratiques différenciées sont des réponses de circonstance pour palier le manque de ressources. Pour plusieurs interlocuteurs, ces pratiques sont connues de la CPS et de fedpol. Dans le premier cas, les experts consultés jugent la pratique non conforme au CPP.

Recherches actives (plateforme *peer to peer*, réseau KIK et enquêtes sous couverture)

Héritage du SCOCI, l'IFC 4/5 collecte des données via la détection automatique sur les plateformes *peer to peer* (P2P) et sur la messagerie KIK[27], et par la recherche active (enquête sous couverture). Comme dans le cas précédent, ce travail donne lieu à des dénonciations aux polices cantonales : 370 en 2019, contre 175 en 2018. Ce bond provient des canaux KIK et P2P ainsi que, dans une moindre mesure, de la reprise d'enquêtes sous couverture en 2019 (graphique 4). Les cantons visités estiment que la qualité de ces dossiers est supérieure à celle des annonces NCMEC.



Graphique 4 – Type de recherches actives réalisées (source : fedpol)

Avec le nouveau CPP en 2011, fedpol ne pouvait plus réaliser d'enquêtes sous couverture en dehors d'une procédure pénale. Le SCOCI et le canton de Schwytz ont trouvé un accord de circonstance basé sur la loi cantonale sur la police. Financé à deux tiers par les cantons, le personnel du SCOCI enquêtait sur mandat de la police schwytzoise comme « agent infiltré » sur les forums Internet. Cette solution se justifiait aussi car la plupart des cantons n'avaient ni base légale, ni ressources, ni compétences pour ces enquêtes.

Entre 2014 et 2020, via ses recherches actives, l'IFC 4/5 a dénoncé 127 personnes auprès des cantons, soit une moyenne de 18 cas par an (annexe 6). En 2018, un seul cas a été transmis. Cette baisse résulte d'un arrêt des enquêtes durant neuf mois. Le chef de la PJF explique cet arrêt en raison d'un changement des cadres à l'IFC 5, mais aussi par une perte de contact et de confiance avec la police cantonale schwytzoise. Cette situation a conduit à la suspension de l'accord, avant que la confiance ne se rétablisse fin 2018.

Lors de l'audit, les cantons de BE et de ZH menaient ce type d'opérations. Le 12 novembre 2020, la CCDJP et la CCPCS ont approuvé une convention administrative sur l'organisation et le financement du NEDIK[28]. Selon un communiqué de presse, les recherches actives – monitoring des réseaux P2P et enquêtes secrètes en l'absence de soupçons – iront aux cantons au 1er janvier 2021. A cet égard, le canton de BE assumera les tâches opérées par l'IFC 4/5 jusqu'ici. Sur mandat du NEDIK, fedpol continuera de traiter et de trier les annonces de soupçons des autorités partenaires étrangères – comme celles de type NCMEC – afin que les parquets des cantons puissent engager une procédure dès qu'un soupçon est confirmé.

Suivi des dénonciations pénales transmises au canton

Le commissariat IFC 4/5 n'a pas de suivi systématique des cas dénoncés aux cantons pour les annonces internationales et les recherches actives (nombre de perquisitions, de condamnations, du montant des amendes, respectivement des jours-amendes, etc.). Par le passé, le rapport annuel du SCOCI incluait des statistiques basées sur le *feedback* des can-

27 KIK Messenger est une application gratuite de messagerie instantanée pour appareils mobiles.
28 CCDJP, *Renforcement des efforts cantonaux contre la cybercriminalité et la pédocriminalité*, 17 novembre 2020.

tons (polices et parquets) et donnait une vue d'ensemble des mesures prises contre la cyber-pédocriminalité[29]. Le SCOCI s'assurait de la sorte du bon déroulement des enquêtes au niveau des délais et sur le plan technique dans le cadre de ses activités de coordination.

La pédocriminalité est de compétence cantonale. La PJF a toutefois le droit de suivre les cas dénoncés, sans contraindre les cantons[30]. Elle a d'ailleurs pu rédiger deux rapports d'analyse sur la lutte contre la cyber-pédocriminalité grâce aux informations cantonales[31]. Ces rapports ne comportent pas un volet lié au suivi des dénonciations. La PJF pense qu'un monitoring de ses activités de coordination permettrait une mesure d'impact *(outcome)*.

Appréciation

La fin de la convention SCOCI entre les cantons et le DFJP ainsi que la reprise des recherches actives en matière de cyber-pédocriminalité proposée par la CCPCS dès le 1er janvier 2021 sont une clarification bienvenue dans la répartition des compétences entre fedpol et les cantons. Ce sera désormais aux cantons d'assurer les ressources nécessaires et l'efficacité de cette lutte contre la pédocriminalité. L'arrêt des recherches actives à l'IFC 4/5 pourrait permettre à la PJF de renforcer sa capacité d'analyse et de tri des annonces NCMEC.

Cette clarification met aussi fin à un système de circonstance avec les autorités schwytzoises qui, bien que performant, avait subit un coup d'arrêt durant neuf mois. Cet arrêt a mis en péril de manière prolongée la mission d'enquête sous couverture de fedpol dans le cadre de la convention SCOCI, tâche financée par les cantons.

Dès 2018, la PJF a pris l'initiative bienvenue de rédiger deux rapports sur la lutte contre la cyber-pédocriminalité. Ce travail devrait se poursuivre. Le processus d'assurance-qualité sur les informations issues des cantons doit cependant être renforcé.

Enfin, la PJF doit prévoir un suivi de ses dénonciations aux cantons ainsi qu'une assurance-qualité sur les données obtenues de ces derniers. Ce suivi entre dans les missions définies par l'Ordonnance sur l'exécution de tâches de police judiciaire à l'Office fédéral de la police. Il permettrait aussi de renforcer la vue d'ensemble sur les phénomènes liés à la cybercriminalité et leur analyse, telle que souhaitée dans la mesure M18 de la SNPC II. Cette amélioration de la traçabilité offrirait enfin une garantie que la Suisse lutte efficacement contre la cyber-pédocriminalité à l'égard de ses partenaires étrangers. La recommandation 4 intègre cet élément d'amélioration.

Encadré 4 – L'outil PICSEL, prometteur pour lutter contre la cybercriminalité

La cybercriminalité est un défi majeur pour la coordination des autorités de poursuite pénale cantonales et fédérales. Celles-ci n'ont pas de vue d'ensemble des phénomènes de criminalité numérique. Dans les cas des cyber-escroquerie par exemple (petites annonces, annonces immobilières, *money mules*, etc.), il est fréquent que les polices cantonales enquêtent contre une personne inconnue, responsable des délits dans plusieurs cantons, alors que les parquets multiplient des réquisitions auprès des mêmes autorités et intermédiaires financiers. Pour améliorer la situation, la mesure M18 de la SNPC II veut une vue d'ensemble (chapitre 4.1). Le projet-phare est la base de données PICSEL qui vise à détecter des séries criminelles dès le dépôt d'une plainte liée à un cyberdélit.

29 Par exemple : SCOCI, Rapport annuel 2013, p. 23-27.
30 Ordonnance sur l'exécution de tâches de police judiciaire à l'Office fédéral de la police, article 4. al. 1 let a.
31 *Pädosexuelle Kriminalität im virtuellen Raum*, juin 2019 et mars 2020.

Créée et utilisée en Suisse romande, PICSEL est en test à la PJF (IFC 4/5) depuis le 1er novembre 2019 et outre-Sarine (BE, ZH, AG). Tous les acteurs – cantons, fedpol, CCPCS et CPS – jugent positifs les premiers retours sur PICSEL. Une centaine de séries criminelles ont pu être détectées sur un volume de plus de 6000 affaires et fedpol l'utilise désormais dans l'analyse des cas de *phishing* (chapitre 2.4). La phase pilote se termine fin 2020.

Lors de l'audit, une minorité des cantons utilisaient PICSEL. De façon transitoire, en attendant que tous les cantons remplissent cette tâche, fedpol s'est proposée comme unité de saisie pour les cantons qui ne participent pas encore au projet. Cette amélioration doit permettre de créer une base de données unifiée et exhaustive au plan suisse. Les détails de cette collaboration doivent être fixés afin que fedpol reçoive les données des cantons concernés dans les délais et puisse aussi garantir l'assurance-qualité lors de la saisie. L'absence de base légale pour l'échange de données entres les cantons et la Confédération reste un défi. Enfin, PICSEL – basé sur le logiciel FileMaker – devrait être initialisé en janvier 2021 en tant que projet d'Harmonisation de l'informatique policière Suisse (HPI). La CCPCS, fedpol et les cantons visités notent que l'idée de PICSEL va dans la bonne direction et que les aspects technologiques ne sont pas un frein.

3.3 Des synergies à l'achat et à l'utilisation des moyens forensiques

La Confédération et les cantons dépensent plusieurs millions de francs par an en matériels et logiciels forensiques IT ainsi que des cours de formations chez une société grisonne. De janvier 2018 à juin 2020, au moins cinq unités fédérales ont acquis pour 1,9 million de francs de *software* et de licences, dont 1,3 million (67,5 %) à cette même société[32]. Le CDF constate que fedpol a une délégation d'achat de l'OFCL pour ces acquisitions essentielles.

Le propriétaire de la société a indiqué au CDF que 80 % de son chiffre d'affaires annuel était réalisé avec les autorités fédérales et cantonales. Cette situation peut être vue comme une position de quasi-monopole, mais rien n'interdit selon lui à ses clients publics d'acquérir ces biens et services en direct auprès des producteurs à l'étranger.

Tous les cantons visités par le CDF achètent des prestations à cette société sans analyse de marché. Aucune police n'envisage d'acquisitions à l'étranger. Les interlocuteurs du CDF s'accordent sur le fait que ces démarches cantonales d'achat n'incitent pas à économiser, y compris dans les frais de formation. Un expert en investigation numérique estime que la Suisse achète trop de licences sans analyse coût-utilité et qu'une centralisation des outils au plan régional permettrait des économies. La CCPCS n'a jamais traité cet aspect.

Des synergies existent parfois. Dans ses prestations forensiques IT, l'IFC peut pénétrer et préserver le contenu de supports mobiles. Cette prestation est réalisée pour d'autres unités fédérales comme l'AFD, mais ce n'est pas systématique pour toute l'administration. L'IFC accomplit aussi cette opération pour les cantons et leur facture le coût lié aux seules licences d'utilisation. Dans un autre domaine, fedpol utilise ponctuellement une prestation auprès du canton de SG. En effet, celui-ci possède un outil d'analyse des ordinateurs de véhicules. Ces exemples de synergies restent toutefois assez rares.

[32] Outre fedpol, le MPC, l'Office fédéral des constructions et de la logistique (OFCL), l'Administration fédérale des douanes (AFD) et la Commission fédérale des maisons de jeu (CFMJ) acquièrent des prestations chez ce fournisseur.

Appréciation

La dépendance des autorités fédérales et cantonales de poursuite pénale à un seul prestataire de biens et de services forensiques est un risque conséquent. Il y a aussi une source d'inefficacité liée au fait que ces autorités réalisent séparément des procédures d'achats identiques pour ces prestations (matériel, logiciels, licences et formation). Ces démarches sont faites sans coordination, ni discussions sur de potentielles économies.

La collaboration entre fedpol et l'AFD doit être encouragée à l'échelle de toute l'administration fédérale. La création d'un centre de compétences, notamment dans le domaine forensique, pour répondre aux besoins d'autres unités de la Confédération serait la bienvenue. Il convient d'examiner comment mettre sur pied un tel centre au sein de fedpol tout en analysant comment compartimenter les données d'enquêtes provenant de différentes administrations fédérales.

Recommandation 6 (Priorité 1)

Le CDF recommande à fedpol, en coordination avec l'OFCL, d'élaborer et de mettre sur pied un centre de compétences forensiques pour l'administration fédérale. Les travaux d'élaboration doivent en particulier tenir compte des questions d'achats (analyse coûts-utilité, économies potentielles) et juridiques liées à la compartimentation et à la protection des données traitées par ce futur centre de compétences.

Prise de position de fedpol

Eine entsprechende Initiative zur Nutzung von Synergien und zur Optimierung der Beschaffungs-Abläufe für sicherheitsrelevante Güter wurde im Sommer 2020 unter Federführung des BBL, zusammen mit dem VBS und der EZV initiiert. Über den Projektfortschritt wird der EFK Bericht erstattet.

4 Le volet pénal de la Stratégie nationale de protection contre les cyberrisques

4.1 Des cyberrisques dans le champ pénal restent à identifier

Le 18 avril 2018, le Conseil fédéral a adopté la SNPC II pour 2018–2022. Lors des entretiens, les autorités de poursuite pénale cantonales et fédérales jugent que cette stratégie constitue une amélioration par rapport à la situation ultérieure. A l'inverse de la première stratégie (2012–2017), la SNPC II intègre une analyse des risques du domaine pénal et comprend quatre mesures pour lutter contre ce type de criminalité. De façon succincte, voici les risques identifiés dans la SNPC II et les mesures adoptées pour les couvrir (M18 à M21)[33] :

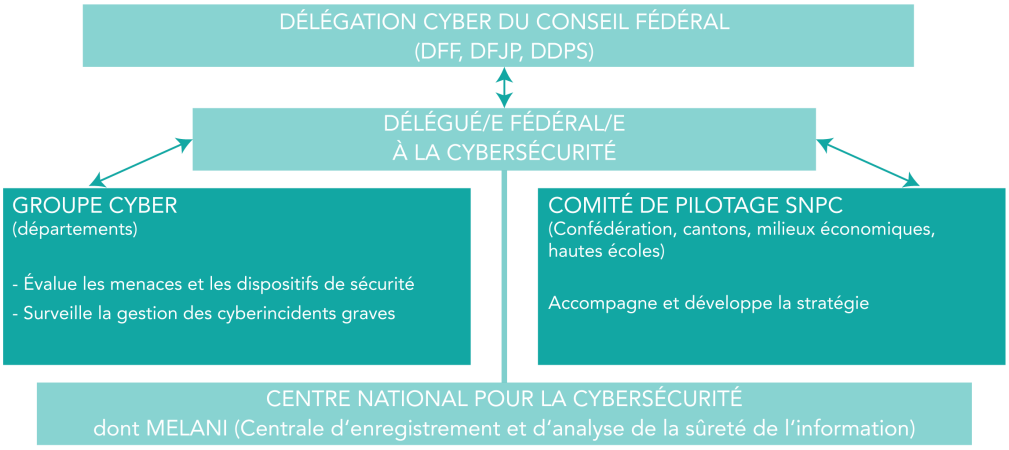
Risques (détectés en 2018)	Mesures et projets à mettre en œuvre (d'ici à 2022)
Les autorités suisses de poursuite pénale ont une vue partielle des infractions liées à la cybercriminalité et une analyse limitée de son évolution.	M18 – La Confédération (fedpol) et les cantons (CCPCS) étudient et conçoivent un cadre technique pour une vue d'ensemble des infractions en matière de cybercriminalité. Trois projets sont lancés : regrouper les données policières dans la base PICSEL ; élaborer un outil de saisie des affaires judiciaires de cybercriminalité en suspens dans les cantons et présenter l'essor du *cybercrime* et ses conséquences.
La collaboration et la coordination entre les autorités de poursuite pénale sont insuffisamment clarifiées entre les acteurs fédéraux et cantons ainsi qu'entre les cantons eux-mêmes.	M19 – La Confédération (fedpol) et les cantons (CCPCS) élaborent le cadre de la collaboration et de la coordination entre les centres de cybercompétences national et cantonaux du réseau de soutien aux enquêtes relatives à la cybercriminalité (réseau NEDIK). Soit fixer les bases légales pour la collaboration et les prestations entre la Confédération et les cantons ainsi qu'au sein des cantons.
Le niveau de formation du personnel des autorités suisses de poursuite pénale n'est pas optimal pour lutter contre la cybercriminalité.	M20 – La mise en œuvre de programmes de formation (modèle à 5 échelons), définis en collaboration par la CCPCS (y compris fedpol) et par la CPS (y compris le MPC), pour l'acquisition de connaissances durables par les autorités de poursuite pénale dans le domaine de la cybercriminalité.
fedpol ne possède pas un office central de police pour lutter contre la cybercriminalité et ses relations avec les cantons demandent des clarifications légales.	M21 – La préparation et l'adoption d'une modification de la loi fédérale sur les Offices centraux de police criminelle[34]. But : créer un office central de lutte contre la cybercriminalité et des bases légales pour la collaboration avec les cantons dans le cadre de cette lutte. fedpol et l'OFJ sont compétents.

Tableau 1 – Risques et mesures dans le champ pénal de la SNPC II et de son plan de mise en œuvre (présentation CDF).

[33] L'annexe 3 présente en détail les mesures 18 à 21, qui en a la responsabilité et le calendrier de mise en œuvre.

[34] Loi fédérale sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres Etats (LOC), RS 360.

Dès l'entrée en vigueur de l'ordonnance sur les cyberrisques le 1er juillet 2020[35], le Centre national pour la cybersécurité (NCSC) coordonne la mise en œuvre de la SNPC II et en effectue un contrôle de gestion stratégique (voir infographie 1). Ce centre est dirigé par le Cyberdélégué de la Confédération, nommé le 14 juin 2019 par le Conseil fédéral. Par ailleurs, le Cyberdélégué est chargé de veiller à une coordination optimale des travaux interdépartementaux des domaines de la cybersécurité, de la cyberdéfense et de la poursuite pénale de la cybercriminalité. Enfin, il préside le Groupe Cyber. Ce Groupe Cyber doit, entre autres, évaluer en permanence les dispositifs existants dans les domaines de la cybersécurité, de la cyberdéfense et de la poursuite pénale de la cybercriminalité et vérifier leur adéquation à la situation et aux objectifs fixés dans la SNPC II. Dans le cas de la poursuite pénale, le Groupe Cyber échange avec le Cyberboard, organe de coordination des procureurs suisses pour les questions de cybercriminalité.



Infographie 1 – Organisation générale de la Confédération dans le domaine des cyberrisques (source : DFF, illustration CDF)

Les cyberrisques sont évalués de manière permanente. Durant les entretiens et sur la base de l'analyse documentaire, il est apparu que cette appréciation en matière de cybercriminalité pouvait être complétée :

- Vue d'ensemble des cyber-infractions : en l'état, la M18 ne parvient pas à produire une image exacte de la nature et du nombre d'infractions liées à cette criminalité. L'analyse des phénomènes risque d'être partielle. En effet, la Suisse ne connaît pas une obligation d'annoncer les cyber-attaques auprès des autorités de poursuite pénale. A de rares exceptions , les entreprises rechignent à porter plainte en cas d'attaques. Dans des cas, des experts évoquent la crainte du dégât d'image ou les difficultés de mener à terme une procédure pénale contre les auteurs de ces cyber-attaques. En dehors du cadre pénal, comme dans le domaine de la surveillance financière par exemple, la Loi fédérale sur l'Autorité fédérale de surveillance des marchés financiers (LFINMA) impose aux intermédiaires financiers de déclarer la survenue d'incidents liés à la sécurité des infrastructures informatiques . Des experts en criminalité numérique et plusieurs acteurs de la poursuite pénale se sont unanimement exprimés pour cette obligation d'annonce sous forme d'un dépôt de plainte. Pour eux, cette obligation améliorerait la fiabilité des

[35] Ordonnance sur les cyberrisques (OPCy), RS 120.73. Avant cette date, cette tâche était assumée par l'Unité de pilotage informatique de la Confédération (UPIC).

statistiques de la cybercriminalité, la qualité de l'analyse et le calibrage des mesures préventives. Cette obligation existe déjà dans les pays de l'Union européenne. Le 11 décembre 2020, le Conseil fédéral s'est dit favorable à une telle obligation pour les seules infrastructures critiques en Suisse . Il a chargé le Département fédéral des finances (DFF) d'élaborer un projet en ce sens qui sera mis en consultation.

- Collaboration au plan international : la position de la Suisse apparaît peu claire dans le cadre de partenariats avec des organisations comme Europol et Interpol, en particulier lorsqu'il s'agit d'apporter son soutien à des actions coordonnées.

Appréciation

Réalisée en 2018, l'analyse des risques pénaux de la SNPC II aborde des points essentiels. L'évolution est positive par rapport aux travaux très peu poussés de la SNPC I. L'analyse des cyberrisques liés à la poursuite pénale en font désormais partie intégrante.

La vue d'ensemble des phénomènes liés à la cybercriminalité mérite d'être complétée, car elle sous-évalue les cyberattaques dont sont victimes les acteurs économiques. Pour différentes raisons, ces acteurs hésitent à porter plainte. Avant de déposer une plainte pénale, rien ne les obligent non plus à communiquer ces incidents aux autorités.

En effet, une obligation de déclarer les défaillances existe pour certains secteurs, mais pas d'obligation générale dans le cas des cyberattaques. L'échange d'informations sur les cyberattaques visant les infrastructures critiques – approvisionnement énergétique, télécommunications, secteur financier, assurances… – s'effectue d'abord sur une base volontaire par l'intermédiaire du NCSC.

Fin 2020, le Conseil fédéral a amorcé de premiers travaux pour obliger de signaler les cyberattaques dans le secteur des infrastructures critiques : c'est un pas dans la bonne direction. Plusieurs acteurs de la poursuite pénale et des experts du domaine estiment que cette obligation devrait s'étendre à l'ensemble des acteurs économiques. Selon le CDF, cette extension permettrait aussi de produire une vue plus complète et une analyse plus exhaustive de la cybercriminalité en Suisse, ce qui est l'objectif de la mesure M18 de la SNPC II.

Il est essentiel pour les autorités suisses de poursuite pénale de pouvoir collaborer aux actions coordonnées au plan international. Les informations sur les attaques cyber en Suisse revêtent également une importance cruciale pour une action cohérente et participative à l'égard de ses partenaires étrangers. L'effort consenti doit donc être poursuivi pour montrer que la Suisse reste un partenaire incontournable.

4.2 Des mesures très générales, sans indicateur de performance

L'analyse des documents montre que les mesures M18 à M21 revêtent un caractère parfois général. C'est aussi le cas pour les buts à atteindre par ces mesures ou par leurs projets. En termes de suivi, ces mesures et leur réalisation sont liées par un calendrier propre rattaché à chaque mesure ou à chaque projet *(milestone)*. En revanche, la SNPC II ne comporte pas un processus formalisé de mise en œuvre avec des indicateurs clé de performance (ou Key Performance Indicators – KPIs).

Par exemple pour le domaine de la formation (M20), le seul projet se résume à la « mise en œuvre du modèle à 5 échelons » (encadré 5). Fin 2019, un « aperçu des possibilités de formations académiques policières » doit être réalisé et « des offres de formation des hautes

écoles spécialisées utilisables par la police » est prévue fin 2020. Aucune autre indication ne permet d'évaluer le niveau requis pour ces formations, le nombre de policiers concernés, les objectifs à atteindre en termes de personnes effectivement formées, etc.

Les services du Cyberdélégué vérifient le respect du calendrier de mise en œuvre et publient un rapport d'avancement[36]. Pour les M18 à M21, le CDF a constaté que lors de l'audit, les appréciations étaient à jour sur la documentation interne[37]. Ces appréciations résultent d'un travail de collecte d'informations auprès des parties prenantes à la SNPC II. Lors de l'audit, le Cyberdélégué estimait que les M18 (Vue d'ensemble de la cybercriminalité, PICSEL) et M20 (Formation) avançaient selon l'échéancier. La M19 (Réseau NEDIK) paraissait être en retard sur le calendrier, alors que la M21 (Bases légales, LOC) serait en avance.

Les entretiens avec le CDF ont montré que les services du Cyberdélégué font confiance à la qualité des informations livrées par leurs partenaires. Ces services ne réalisent pas d'examen critique des *reportings* sur l'avancement des mesures M18 à M21. Aucun outil n'offre au Cyberdélégué la possibilité d'apprécier pleinement si un *milestone* est déjà respecté, le sera selon le calendrier ou ne le sera pas. Lors des entretiens, le Cyberdélégué a montré une adaptation du processus de monitoring de la SNPC II avec des niveaux de maturité actuels et escomptés pour chaque mesure[38]. Dans l'idéal, ce dispositif devrait être complété par l'élaboration de KPIs pour toutes les mesures de la SNPC II. Il souhaite aussi améliorer l'information aux décideurs, notamment dès 2022 dans le cadre de la future SNPC III.

Appréciation

L'évaluation du Cyberdélégué sur l'état d'avancement des M18 à M21 est en partie confirmée par les résultats du CDF sur le terrain. La mise en place du réseau NEDIK (M19) connaît des retards (encadré 2), tandis que la LOC (M21) semble avancer à bon rythme sous réserve d'un référendum (chapitre 3.1). Le CDF est moins optimiste quant à la mise en œuvre d'une partie des formations sur le terrain (M20, encadré 5), alors que la création de la vue d'ensemble avec la base PICSEL semble suivre le calendrier (M18, encadré 4). Cette appréciation différenciée montre un problème de fond.

Le suivi des mesures par les services du Cyberdélégué présente le risque de ne pas apprécier la réalité de la situation et le chemin à parcourir pour pleinement remplir les objectifs de la Stratégie. Les autorités politiques – le Conseil fédéral et le Parlement – ne possèdent pas encore les moyens adéquats, ni l'information pertinente pour suivre entièrement l'avancement réel de la Stratégie et orienter les options d'une future SNPC III.

Conscient de cette situation, le Cyberdélégué a procédé à une première adaptation courant 2020. Cela démontre le besoin de formaliser ce processus de monitoring. Cette adaptation reste toutefois insuffisante pour garantir la réalisation pleine et entière des mesures de la SNPC II suivant le calendrier fixé.

Le CDF estime qu'un système d'indicateurs de performance est nécessaire pour crédibiliser le suivi des mesures. Si une hypothétique SNPC III devait voir le jour dès 2023, il conviendrait que le Cyberdélégué dispose de mesures précises, sujettes à une assurance-qualité et évaluables dans le temps, autant pour la lutte contre la cybercriminalité que les autres do-

[36] Le dernier Rapport sur l'avancement des travaux concernant la SNPC (2018–2022) a été publié le 19 octobre 2020.
[37] Strategisches Meilensteincontrolling NCS-Umsetzung 2018–2022
[38] Ist-Zustand und Ambitionsniveau NCS-Beschlüsse vom 29.06.2020.

maines de la Stratégie. Un système d'indicateurs de performances devrait aussi lui permettre de renforcer ses moyens de contrôle. Il devrait encore permettre d'améliorer et de formaliser significativement la transmission et l'échange des informations. Enfin, ces différentes mesures permettront au NCSC d'améliorer la pertinence de ses rapports d'avancement de la SNPC à l'attention des décideurs politiques fédéraux et cantonaux.

Recommandation 7 (Priorité 1)

Dans le cadre des travaux de la future Stratégie nationale de protection contre les cyberrisques (SNPC III), le CDF recommande au Centre national pour la cybersécurité d'élaborer un système d'indicateurs de performance (KPIs) pour évaluer l'efficacité de chacune des mesures qui y sera définie.

Prise de position du SNPC

Die Ermöglichung einer Wirksamkeitsmessung mittels Leistungsindikatoren wird bei der Erarbeitung der neuen NCS entsprechend berücksichtigt.

Encadré 5 – Formation des policiers à la cybercriminalité (M20)

Deux cantons ont indiqué au CDF des pratiques différenciées chez les policiers – plus de 16 000 personnes – qui ont suivi le module *e-learning* du degré I de formation. Selon eux, des stratégies différenciées de formation existent, par exemple, selon l'âge du personnel de police (exemption pour des policiers proches de la retraite). Des variations sur la durée consacrée à ces cours ont aussi été signalées, comme des temps de réponses au test parfois très courts (utilisation de *check-lists*). Pour le deuxième échelon de formation, deux cantons jugent trop ambitieux de former leurs enquêteurs judiciaires dans un délai de moins de deux ans. Un délai de dix ans semblerait plus atteignable. Des interlocuteurs cantonaux relèvent que la M20 instaure des programmes, mais ne fixe pas d'objectifs à atteindre en termes de policiers formés à la lutte contre la cybercriminalité, ni une planification pour y parvenir. La définition d'un processus d'assurance-qualité garantirait que tous les bénéficiaires de cours s'astreignent à les suivre dans les durées d'enseignement et d'évaluation fixées. Portés à la connaissance du CDF, ces éléments lui font relativiser l'appréciation du Cyberdélégué selon laquelle la mise en œuvre de la M20 avancerait selon le calendrier fixé.

Annexe 1 : Documents officiels

Textes législatifs
Code pénal (CP)
Code de procédure pénale (CPP)
Loi fédérale sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres États (LOC), RS 360
Loi fédérale sur les systèmes d'information de police de la Confédération (LSIP), RS 361
Loi fédérale sur les mesures policières de lutte contre le terrorisme (MPT), approuvée par les Chambres fédérale, soumise au délai référendaire
Message du Conseil fédéral concernant la loi fédérale sur les mesures policières de lutte contre le terrorisme (MPT), Feuille fédérale, 2019
Ordonnance concernant l'exécution de tâches de police judiciaire au sein de l'Office fédéral de la police, RS 360.1
Ordonnance sur la protection contre les cyberrisques dans l'administration fédérale (Ordonnance sur les cyberrisques, OPCy), RS 120.73
Documents officiels
Administration fédérale des finances, Compte d'Etat 2019, tome 2
BRB, Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022, 18 avril 2018
BRB, Umsetzungsplanung Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022, 15 mai 2019
BRB, Bericht über die Organisation des Bundes zur Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken, 25 février 2020
Convention administrative entre le Département fédéral de justice police (DFJP) et la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP), 19 décembre 2001
CDF, Prüfung der Aufsicht über die Cybersicherheit bei Finanzdienstleistern, PA 20013
Cyberdélégué, Ist-Zustand und Ambitionsniveau NCS-Beschlüsse vom 29. Juni 2020
Cyberdélégué, Strategisches Meilensteincontrolling NCS-Umsetzung 2018–2022

Cyberdélégué, Rapport sur l'avancement des travaux concernant la SNPC (2018–2022), 19 octobre 2020

Eidgenössisches Finanzdepartement, Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen – Rechtliche Grundlagen, 11 Dezember 2020

fedpol, Pädosexuelle Kriminalität im virtuellen Raum, Juni 2019

fedpol, Pädosexuelle Kriminalität im virtuellen Raum, März 2020

fedpol, Rapport annuel du SCOCI, 2013

MPC, Concept sur la délimitation des compétences dans le domaine de la lutte contre la cybercriminalité, 2018

MPC, Massnahmenempfehlungen Cyberkriminalität bis 2023 – Validiert durch GL am 29. April 2019

MPC, Umsetzungsplan – Cybercrime, Juni 2020

Interventions parlementaires

Proposition M. Meyer, Budget de la Confédération 2020 assorti du plan intégré des tâches et des finances 2021–2023 (19.041)

Annexe 2 : Abréviations

AC	« Analyse criminelle », division de la PJF
AFD	Administration fédérale des douanes
BKP	Bundeskriminalpolizei (PJF, en français)
CAS	Certificate of Advanced Studies
CCC	Convention sur la cybercriminalité de Budapest
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
CCPCS	Conférence des Commandants des Polices Cantonales de Suisse
CDF	Contrôle fédéral des finances
CFMJ	Commission fédérale des maisons de jeu
CLEMONA	Application pour automatiser le traitement des informations entrantes au niveau de la coopération policière, fedpol
CP	Code pénal suisse
CPP	Code de procédure pénale
CPS	Conférence des procureurs suisses
DFF	Département fédéral des finances
DFJP	Département fédéral de justice et police
EIMP	Entraide internationale en matière pénale
ErmSys	Ermittlungssystem
ETP	Equivalent Temps Plein
FAP	Feinauswertungsplattform
fedpol	Office fédéral de la police
GPS	Global Positioning System
IFC	« IT Forensique & CyberCrime », division de la PJF

ISP	Institut suisse de police
ISS	Système d'interceptions téléphoniques
IT	Information Technology
KIK	Système de messagerie électronique
KPIs	Key Performance Indicators
LFINMA	Loi fédérale sur l'Autorité fédérale de surveillance des marchés financiers
LOC	Loi fédérale sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres Etats
LSI	Projet de loi sur la sécurité de l'information
MPC	Ministère public de la Confédération
MPT	Projet de loi fédérale sur les mesures policières de lutte contre le terrorisme
NC3	Centre de compétences national en matière de cybercriminalité, fedpol
NCMEC	National Center for Missing and Exploited Children
NCSC	Centre national pour la cybersécurité, DFF
NEDIK	Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung
OFCL	Office fédéral des constructions et de la logistique
OFS	Office fédéral de la statistique
OPGKBKP	Operative Geschäftskontrolle BKP
ORMA	Application de gestion et de suivi des dossiers de la PJF
PICSEL	Plateforme d'Information de la Criminalité Sérielle En Ligne
PJF	Police judiciaire fédérale
PT / CATS	Personnel Time Management / Cross-Application Time Sheet
P2P	Peer to Peer (plateforme d'échanges informatiques)

RC3	Centres régionaux de compétences en matière de cybercriminalité (en cours de création)
RTV	« Entraide judiciaire, terrorisme et droit pénal international », division de la PJF
RTVC	« Entraide judiciaire, Terrorisme, Droit pénal international, Cyber », division du MPC
SCOCI	Service de coordination de la lutte contre la criminalité sur Internet
SNPC	Stratégie nationale de protection contre les cyberrisques
TPF	Tribunal pénal fédéral
UPIC	Unité de pilotage informatique de la Confédération
WK	« Criminalité économique », division de la PJF

Priorités des recommandations

Le Contrôle fédéral des finances priorise ses recommandations sur la base de risques définis (1 = élevés, 2 = moyens, 3 = faibles). Comme risques, on peut citer par exemple les cas de projets non-rentables, d'infractions contre la légalité ou la régularité, de responsabilité et de dommages de réputation. Les effets et la probabilité de survenance sont ainsi considérés. Cette appréciation se fonde sur les objets d'audit spécifiques (relatif) et non sur l'importance pour l'ensemble de l'administration fédérale (absolu).

Annexe 3 : Mise en œuvre SNPC II (volet pénal)

7.7 Poursuite pénale

Le cyberespace fournit aux criminels potentiels de nouvelles opportunités, susceptibles d'entraîner de sérieux dommages pour la société et l'économie. Les actes ne sont plus véritablement limités dans le temps et l'espace. Dans ce contexte, il faut agir dans toute la Suisse et en collaboration avec des partenaires internationaux afin d'améliorer l'interopérabilité et la capacité de réaction et de coordonner efficacement les compétences professionnelles, techniques et humaines, sans devoir pour autant céder des prérogatives d'une autorité ou d'un niveau étatique à l'autre.
Créé en 2018 pour la coordination nécessaire à cet effet, le Cyberboard permet aux services compétents d'échanger, de développer des stratégies et de se coordonner entre eux au niveau opérationnel.

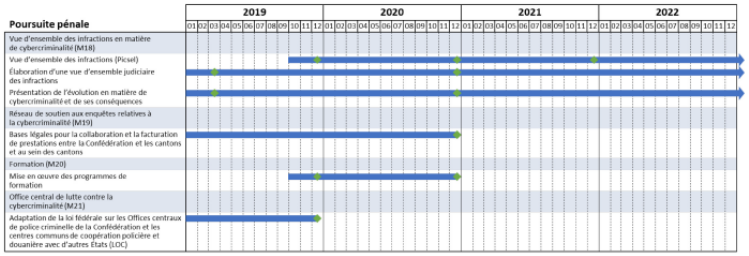


Figure 11: feuille de route «Poursuite pénale»

7.7.1 Vue d'ensemble des infractions en matière de cybercriminalité (M18)

Aperçu de la mesure	
Objectif	La Confédération (fedpol) et les cantons (CCPCS) étudient et conçoivent le cadre technique nécessaire à l'élaboration d'une vue d'ensemble des infractions en matière de cybercriminalité en Suisse (données policières).
Responsabilité	fedpol dans le cadre des activités du Cyberboard
Participation	Cyberboard, Office de l'auditeur en chef / justice militaire / police militaire
Comités / processus / projets	HiP, (Picar-Picsel), NEDIK, Cyber-CASE
Projets de mise en œuvre	1. Vue d'ensemble des infractions (Picsel) 2. Élaboration d'une vue d'ensemble judiciaire des infractions 3. Présentation de l'évolution en matière de cybercriminalité et de ses conséquences

Projets de mise en œuvre

1. Vue d'ensemble des infractions (Picsel)	
Description du projet	Regrouper les données policières au niveau national grâce à Picsel. Processus en trois phases: • Création du cadre technique • Cadre juridique • Utilisation de la vue d'ensemble des infractions
Compétence	fedpol, HiP
Étapes	***T4/2019*** Démarrage de la phase test de Picsel ***T4/2020*** Diffusion nationale par l'intermédiaire des cantons; participation d'au moins 3 concordats ***T4/2021*** Précision du cadre technique ***T4/2023*** LOC en vigueur (au niveau légal) ***T4/2023*** Mise en service de Picsel (données cantonales)

2. Élaboration d'une vue d'ensemble judiciaire des infractions	
Description du projet	Élaboration d'un instrument de saisie, au niveau national, de toutes les affaires de cybercriminalité en suspens dans les cantons (vue d'ensemble intercantonale des infractions)
Compétence	Cyberboard (Cyber-CASE, cantons, MPC et fedpol)
Étapes	***T1/2019*** Outil Cyber-CASE; liste des infractions pour tous les procureurs qui font office d'interlocuteurs uniques dans le domaine de la cybercriminalité (opérationnelle) ***T4/2020*** Outil en ligne pour la vue d'ensemble des procédures en cours ***T1/2021 Combinaison de l'état de la situation selon la police (Picsel) et de la vue d'ensemble judiciaire des infractions***

3. Présentation de l'évolution en matière de cybercriminalité et de ses conséquences	
Description du projet	Développement continu de produits pour la police et la justice (tendances, meilleures pratiques, rapport d'analyse, etc.)
Compétence	Cyberboard (NEDIK), cantons (polices cantonales, ministères publics cantonaux), MPC, fedpol et Office de l'auditeur en chef / justice militaire / police militaire
Étapes	***T1/2019*** Bulletin mensuel (de la police) ***T4/2020*** Vue d'ensemble des procédures en cours (police et justice)

7.7.2 Réseau de soutien aux enquêtes relatives à la cybercriminalité (M19)

Aperçu de la mesure	
Objectif	La Confédération (fedpol) et les cantons (CCPCS) élaborent le cadre de la collaboration et de la coordination entre les centres de cybercompétences national et cantonaux dans le cadre du NEDIK.
Responsabilité	CCPCS
Participation de services fédéraux	fedpol avec le Cyberboard
Participation de tiers	Police cantonale, CCPCS
Comités / processus / projets	Groupe de travail NEDIK
Projets de mise en œuvre	1. Bases légales pour la collaboration et la facturation de prestations entre la Confédération et les cantons et au sein des cantons

Projets de mise en œuvre

1. Bases légales pour la collaboration et la facturation de prestations entre la Confédération et les cantons et au sein des cantons	
Description du projet	Élaboration des bases légales pour la collaboration et la facturation de prestations entre la Confédération et les cantons et au sein des cantons
Compétence	CCPCS et fedpol
Étapes	***T4/2020*** Signature et adoption d'une ou plusieurs conventions

7.7.3 Formation (M20)

Aperçu de la mesure	
Objectif	Des programmes de formation sont spécifiquement définis avec la collaboration de la CCPCS et la Conférence des procureurs de Suisse (CPS), en vue de l'acquisition durable des connaissances nécessaires dans le domaine de la poursuite pénale.
Responsabilité	CCPCS (y c. fedpol), CPS (y c. MPC)
Participation	Cyberboard
Comités / processus / projets	• Groupe de travail sur les formations dans le domaine de la cybercriminalité • Formations existantes (HEG-ARC ERMP) • Académie des avocats (HSLU) • Cyber-CASE
Projets de mise en œuvre	1. Mise en œuvre des programmes de formation

Projets de mise en œuvre

1. Formations	
Description du projet	Mise en œuvre du modèle à 5 échelons -> formations
Compétence	Institut Suisse de Police (ISP), formations du groupe de travail cybercrime
Étapes	***T4/2019*** Aperçu des possibilités de formations académiques (policières) ***T4/2020*** Offres de formation des hautes écoles utilisables par la police

7.7.4 Office central de lutte contre la cybercriminalité (M21)

Aperçu de la mesure	
Objectif	fedpol prépare une modification de la loi fédérale sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres États (LOC) en vue de la création d'un office central de lutte contre la cybercriminalité et des bases légales nécessaires, afin de permettre la collaboration avec les cantons dans le cadre de la lutte contre la cybercriminalité.
Responsabilité	fedpol
Participation	Cyberboard, Office fédéral de la justice
Comités / processus / projets	LOC
Projets de mise en œuvre	1. Adaptation de la loi fédérale sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres États (LOC)

Projets de mise en œuvre

1. Adaptation de la loi fédérale sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres États (LOC)	
Description du projet	Création d'une base légale pour un office central de lutte contre la cybercriminalité Entre autres, réglementation de l'échange de données de la police
Compétence	fedpol et Office fédéral de la justice (OFJ)
Étapes	***T4/2022*** LOC révisée et adoptée

Annexe 4 : Le Parlement renforce la lutte contre la pédocriminalité

Auteure

Mattea Meyer, Nationalrätin (SP/ZH)

Proposition 19.041-1 du 2 décembre 2019

Die im Voranschlag 2020 vorgenommene Aufstockung von 600 000 Franken ist im Personalaufwand zur Verstärkung der Bekämpfung der Pädokriminalität einzusetzen

Développement

Im Rahmen des Stabilisierungsprogramm 2017-2019 reduzierte das fedpol unter anderem den Personalaufwand im Bereich der Koordinationstätigkeit mit den Strafverfolgungsbehörden im In- und Ausland im Bereich der Pädokriminalität/Pornografie.

Die Strafverfolgung der Pädokriminalität liegt im Aufgabenbereich der Kantone. Fedpol nimmt aber sogenannte Zentralstellenaufgaben wahr. Dazu gehört, die Schnittstelle zwischen dem Ausland, Fedpol und den kantonalen Polizeikorps sicher zu stellen. Dank dieser Triage-Funktion entlastet Fedpol die Kantone. Fedpol fungiert zudem als Nationales Kompetenzzentrum für Cybercrime. Die an die Schweiz übermittelten Verdachtsmeldungen auf Kinderpornografie steigen sehr stark an. Dies bedeutet auch einen Mehraufwand bei Fedpol, welches die internationalen Meldungen entgegennimmt, auf Strafbarkeit überprüft und an die Kantonspolizeikorps übermittelt. Ist eine Verdachtsmeldung zudem nicht eindeutig einem Kanton zuweisbar, kann Fedpol selber erste Ermittlungen führen.

Der Einzelantrag verlangt eine Stellenaufstockung von 4 Stellen, um in Zukunft die Zentralstellenaufgaben im Bereich Internetkriminalität, insbesondere im Bereich der Pädokriminalität, zu verstärken und die Kinder besser zu schützen.

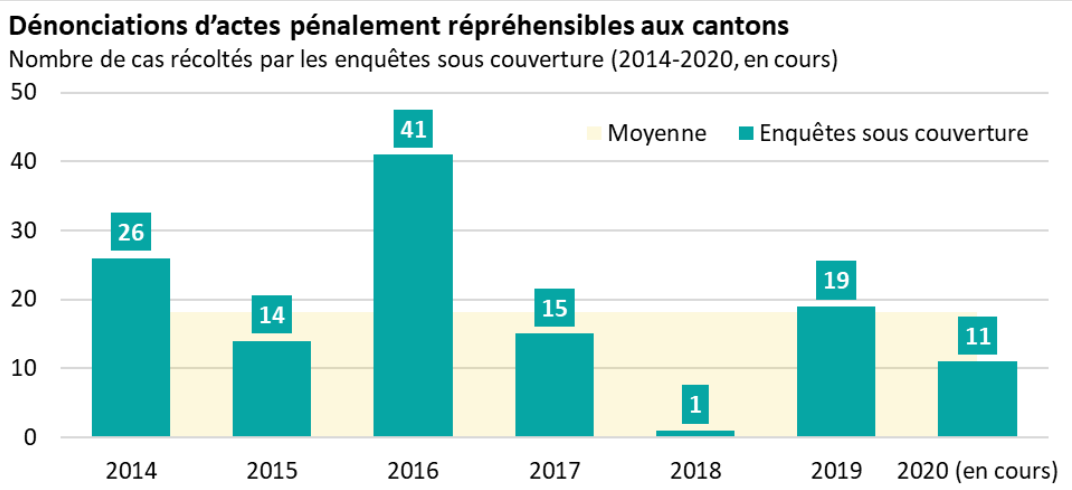
Adoptée par les Chambres fédérales le 5 décembre 2019

Annexe 5 : Documentation postes du Parlement

Type de document	Analyste Police Analyse criminelle, PJF	Conseiller spécialisé I Etat-major, PJF	Conseiller spécialisé I Prévention de la criminalité et État-major de direction	Spécialiste en communication Communication
Proposition	Partiellement signée, scannée (21.2.2020)	Partiellement signée, scannée (21.2.2020)	Entièrement signée et scannée (23.12.2019)	Document Word pas signé. Pas d'autre document scanné.
Description de poste / Cahier des charges	Adéquation à la proposition, mentionne les infractions en ligne (cybercrime) et en particulier de la pédopornographie.	Les documents existent et font référence à la criminalité numérique, mais rien de spécifique à la pédocriminalité.	Pas de description de poste, ni de cahier des charges reçu par le CDF.	Cahier des charges présent, correspond à un emploi de porte-parole. Pas de référence au cybercrime, ni à la pédocriminalité.
« Décision météo »	Document disponible (25.2.2020)	Document disponible (25.2.2020)	Pas de décision documentée	Pas de décision documentée

Tableau 2 – Nature et qualité des documents transmis par fedpol pour les postes du Parlement (source : CDF)

Annexe 6 : Enquêtes sous couverture



Graphique 5 – Dossiers issus des recherches sous couverture grâce à l'accord avec le canton de Schwytz (source : fedpol).