Zeitschrift: Kriminologie / Schweizerische Arbeitsgruppe für Kriminologie SAK = Criminologie / Groupe Suisse de Criminologie GSC = Criminologia / Gruppo Svizzero di Criminologia GSC

Herausgeber: Schweizerische Arbeitsgruppe für Kriminologie

Band: 38 (2021)

Artikel: Les défis de la lutte contre la cybercriminalité

Autor: Fink, Daniel

DOI: https://doi.org/10.5169/seals-1051606

Les défis de la lutte contre la cybercriminalité

Daniel Fink*

Table des matières

Résumé

La poursuite des délits de cybercriminalité représente un véritable défi pour les autorités de poursuite pénale, et ce, sur de nombreux plans. Techniquement, parce que les auteurs d'infractions dans le cyberespace possèdent un haut niveau de maîtrise des nouvelles technologies. Juridiquement, parce qu'ils savent qu'en agissant sur le plan international, ils ralentissent l'action de la justice qui doit recourir à l'entraide judiciaire, tout en sachant que la qualification juridique est complexe. Politiquement, en raison du système fédéraliste suisse des autorités judiciaires. Cette contribution offre un aperçu des défis et difficultés de la poursuite pénale qui, de plus, se déroule dans des conditions-cadres continuellement changeantes.

Zusammenfassung

Die Verfolgung von Straftaten im Zusammenhang mit Cyberkriminalität stellt die Strafverfolgungsbehörden in vielerlei Hinsicht vor eine echte Herausforderung. Technisch gesehen, weil die Täter im Cyberspace über höchste Kompetenzen in neuen Technologien verfügen. Rechtlich gesehen, weil sie wissen, dass sie durch ihr Handeln auf internationaler Ebene das Vorgehen der Justiz verlangsamen, die auf gegenseitige Rechtshilfe zurück-

* Chargé de cours à l'Université de Lucerne et membre associé à l'Ecole des sciences criminelles de l'Université de Lausanne.

greifen muss, wie sie auch wissen, dass die rechtliche Qualifikation komplex ist. Politisch aufgrund des schweizerischen föderalistischen Justizsystems. Dieser Beitrag bietet einen Überblick über Herausforderungen und Schwierigkeiten der Strafverfolgung, die unter ständig neuen Rahmenbedingungen stattfinden muss.

1. Evolution de la cybercriminalité et des premières mesures pour la contrer[1]

On s'accorde généralement à dater l'émergence de la cybercriminalité – c'est-à-dire des infractions commises dans l'espace virtuel de l'échange d'information – au milieu des années 1990, lorsqu'apparaissent l'internet grand public et les premiers systèmes de courriels. En même temps, il faut bien reconnaître que les infractions liées à l'abus de machines connectées de traitement de l'information sont antérieures et datent de l'introduction de la carte de crédit et des premiers grands systèmes informatiques dans les entreprises.

Dès le milieu des années 1990 cependant, un nouveau seuil est franchi, car ce sont maintenant les systèmes informatiques qui sont intentionnellement infectés avec des logiciels malveillants (*malware*) permettant à des intrus malintentionnés d'obtenir l'accès à des ordinateurs, pour les raisons les plus diverses, de l'enrichissement personnel en passant par la volonté de nuire, jusqu'à l'espionnage. Dès cet instant commencent à se multiplier les programmes de protection, et une course entre auteurs d'infractions de cyberdélinquance et producteurs de logiciels de protection s'engage. Ces programmes étaient censés protéger les machines et logiciels des utilisateurs individuels plutôt que des grands systèmes. Dans un premier temps, le problème est réglé dans l'espace privé et commercial plutôt qu'au niveau de la police et de la justice. Peu de temps après, les grandes entreprises, et les moins grandes dans leur sillage, mettent en place des départements et des systèmes de sécurité informatique, en vue de protéger leurs systèmes de plus en plus reliés, voire ouverts à travers internet sur le plan mondial. L'Etat et l'administration suivent, suite notamment aux résultats des travaux de la commission présidentielle américaine (sous la présidence Clinton) sur la protection des infrastructures critiques.

Plus tôt déjà, à savoir dès le milieu des années 1980, ce sont les militaires qui se préparent afin d'être prêts à engager des actions offensives et défensives

1 Procureur au Ministère public de la Confédération, Yves Nicolet a fait une présentation sur le thème de la cybercriminalité lors de la conférence annuelle du Groupe Suisse de Criminologie en 2020, mais n'a pu disposer de suffisamment de temps pour rédiger une contribution pour ces Actes. De ce fait, inspiré par sa conférence et en prolongement d'autres travaux en cours, Daniel Fink a écrit cet article qui expose brièvement l'évolution de divers thèmes sur la cybercriminalité en offrant quelques réflexions critiques.

visant l'information et les infrastructures de la société de l'information, voire les infrastructures critiques. Ainsi, les Etats-Unis, dans la première Guerre du Golfe de 1991, ont très tôt lancé des actions de cyberattaques contre les infrastructures d'information et de communication de leurs adversaires. En 1999, dans la guerre contre la Serbie, les attaques seront également dirigées contre le bon fonctionnement de l'internet ; de nombreuses actions de déni de service ont été lancées contre les systèmes informatiques et de communication. Après cette période offensive, face aux menaces montantes d'autres acteurs capables de lancer des actions nuisibles ou destructrices, se développent aux Etats-Unis, au sein du Département de la sécurité intérieure, les premiers travaux de cybersécurité. Simultanément, l'ONU engage, dès 2003, une réflexion sur le plan mondial sur les enjeux du numérique, y incluant la cybercriminalité et la cybersécurité. En Europe, l'Agence européenne de cybersécurité est créée en 2004.

2. La Suisse se met en marche

En Suisse également, on se met à travailler sur la cybercriminalité, d'abord dans le monde universitaire où a été créée la Fondation SWITCH, acronyme de *Swiss Tele Communication System for Higher Education* qui était, dès octobre 1987, en charge de développer le réseau informatique entre les universités et de gérer le nom de domaine « .ch ». Elle a aussi joué un rôle dans les premières tentatives de lutte contre les *malwares* qui commencent aussitôt à affecter les réseaux d'échange d'information et les ordinateurs.

Sur le plan pénal, le Conseil fédéral avait mandaté un groupe d'experts au début des années 1980 pour élaborer une révision du droit pénal relatif aux infractions contre le patrimoine, notamment en relation avec les infractions à la carte de crédit et certains types d'infractions informatiques[2]. Le législateur l'adopta après avoir apporté de légères modifications aux définitions de ces délits, qui n'étaient pas encore appelés cyberdélinquance ; la révision entra en vigueur en 1995. Il s'agissait notamment des articles suivants :

2 Message du 24.4.1991 concernant la modification du code pénal suisse et du code pénal militaire (Infractions contre le patrimoine et faux dans les titres) (91.032). Les dispositions sur la « soustraction de données » (art. 143bis) protègent des « données enregistrées ou transmises électroniquement ou selon un mode similaire (y compris les logiciels) qui ne sont pas destinées à l'auteur. Elle réprime en outre celui qui s'introduit sans droit dans un système de traitement des données, autrement dit le ‹ piratage › (*Hacken*). Par ailleurs, la disposition sur les dommages à la propriété consacre désormais un alinéa séparé aux dommages occasionnés à des données informatiques. » (936).
Tous les documents cités dans cet article étant accessibles sur le site web de la Confédération par simple introduction du titre ou des numéros de référence dans un moteur de recherche, nous avons renoncé à indiquer les adresses internet et la date d'accès aux documents. Ils ont tous été consultés entre mai et mi-juin 2021.

- Art. 143 CP : Soustraction de données
- Art. 143bis CP : Accès indu à un système informatique
- Art. 144bis CP : Détérioration de données
- Art. 147 CP : Utilisation frauduleuse d'un ordinateur.

Il faut noter que ces dispositions se sont révélées bien conçues, étant donné que la signature de la Convention du Conseil de l'Europe sur la cybercriminalité de 2001 par la Suisse, dans la même année, ne nécessita qu'une révision mineure du droit établi en 1995. La Suisse ne ratifia cette convention qu'en 2010. Dans son message concernant l'adoption de la Convention, le Conseil fédéral déclara laconiquement : « Il faut seulement modifier la définition de l'accès indu à un système informatique (ce que l'on appelle le ‹ piratage informatique ›, art. 143bis du code pénal) en pénalisant des actes commis antérieurement au piratage lui-même »[3]. D'un point de vue juridique, le système pénal était donc en place, et même si les structures de la poursuite institutionnelle étaient aussi dispersées qu'elles doivent l'être dans un état fédéral, cela ne devait pas constituer, comme dans d'autres domaines de délinquance, un obstacle à une poursuite réussie et efficace de ces types d'infraction.

Au tournant du nouveau millénaire, les questions de la cybercriminalité, de l'espionnage informatique et du « hacktivisme » sont considérées comme des menaces en Suisse. La Confédération, à travers l'Office fédéral de la police, se mobilise et, fédéralisme oblige, crée un *Service national de coordination de la lutte contre la criminalité sur Internet* (SCOCI). Trois domaines de responsabilité lui sont attribués : monitorage de l'internet au sujet d'actes punissables, analyse de cas et coordination des procédures d'enquête. Dès 2003, on se félicite qu'il y ait jusqu'à 500 cas par mois qui sont soumis au SCOCI. Le service est réorganisé en 2004 ; l'Office fédéral de la police est désormais chargé de gérer la *Centrale d'enregistrement et d'analyse pour la sûreté de l'information* appelée MELANI, opérationnelle dès octobre 2004. Tout en intégrant certaines des tâches du SCOCI, son mandat est bien plus large et consiste désormais à « faire en sorte que les interruptions du fonctionnement des réseaux et des systèmes, tout comme les usages abusifs, soient rares, brefs et maîtrisables, et que leurs conséquences soient aussi limitées que possible »[4]. On notera le changement de ton qui passe de l'objectif de « lutte contre » à la « limitation des dommages ».

Parallèlement à ces développements, des efforts sont déployés pour la protection des infrastructures critiques, constituées par les équipements tels que la production ou l'acheminement de l'énergie (centrales nucléaires, barrages, gaz, pétrole), le bon fonctionnement des transports et télécommunications, notam-

3 Message du 18.6.2010 relatif à l'approbation et à la mise en œuvre de la convention du Conseil de l'Europe sur la cybercriminalité (10.058), 4276.

4 Communiqué du Conseil fédéral, 2007.

ment le fonctionnement de l'internet lui-même, et des hôpitaux. Alors même que tous les experts semblent s'accorder sur le fait qu'on ne peut séparer les diverses facettes et niveaux d'action pour la cybersécurité d'un pays, « (p)our des raisons d'un (doux) jeu de pouvoir entre départements et des sensibilités politiques générales »[5], les efforts liés à la protection de l'infrastructure virtuelle de l'information, soutenus par MELANI, ont été séparés de ceux devant garantir la protection des infrastructures critiques, tâche qui a été attribuée à l'Office fédéral de la protection civile. Et finalement, un dernier volet concernait l'armée et la cyberdéfense. Suite aux développements de la guerre dans l'espace virtuel mentionnée ci-dessus, on a souhaité, du côté du Département fédéral de la défense, de la protection de la population et des sports, développer cet aspect de la défense nationale. Les travaux entrepris par l'armée aboutissent à la mise en place d'un projet de cyberdéfense, d'abord poursuivi en autonomie, et dès 2018 coordonné dans le cadre de la stratégie nationale de protection de la Suisse contre les cyberrisques.

Avec un nombre croissant de domaines politiques, économiques et administratifs et d'acteurs sociaux concernés par, voire directement confrontés à la cybercriminalité, la Confédération organise les forces et développe une stratégie d'ensemble. Ces efforts aboutissent en 2012 au premier document de stratégie nationale de protection contre les cyberrisques (SNPC), concentré sur le civil, excluant le militaire qui a sa propre logique. Cette stratégie comprend notamment des structures organisationnelles entre l'administration et l'économie et renforce le rôle de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI). Comme dans d'autres domaines, on passe de l'analyse des risques, vulnérabilités et menaces, à la gestion de la continuité et des crises, avec notamment le « renforcement et l'amélioration de la capacité de résistance (résilience) face aux dérangements et événements imprévus » (DFF, SNPC, 2013). Si le document de 2013 compte sept champs d'action, et 16 mesures concrètes à mettre en œuvre jusqu'en 2017, le plan pour la période de quatre ans 2018-2022 comprendra quant à lui dix champs d'action, 29 mesures et 247 étapes de mise en œuvre. Alors que dans le premier document, la poursuite pénale n'était pas explicitement mentionnée, elle l'est à partir de 2018 : « Ce domaine comprend l'ensemble des mesures de la police et des ministères publics de la Confédération et des cantons pour lutter contre la cybercriminalité »[6]. Il est intéressant de noter qu'au moment même où toute la Confédération est astreinte au plan de limitation du personnel, le domaine de la cybersécurité obtient 30 postes, et est augmenté ensuite de 67 postes pour la période de 2018 à 2022[7].

5 Myriam Dunn Cavelty, Cybersecurity in Switzerland, Berlin 2014, 19.

6 Rapport du 27.11.2019 sur l'organisation de la Confédération pour la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques, ici 7.

7 *Idem*, 13.

3. Une statistique de la cybercriminalité – un projet inachevé

Comme son nom l'indique, et comme les premiers travaux de définition relatifs à la cybercriminalité le confirment, on parle dans ce domaine d'une gamme large et variée d'infractions, impliquant une grande diversité de personnes et d'entités potentiellement ou réellement lésées, tout comme une multitude de modes opératoires. En 2010, le message du Conseil fédéral en vue de la ratification de la première convention européenne du Conseil de l'Europe relative à la cybercriminalité constatait que l'arsenal juridique pour la poursuite pénale était à la hauteur de l'enjeu, mais qu'on avait une bien piètre idée du volume et de la diversité de ces infractions commises dans l'espace virtuel. Du côté de MELANI, on notait que les chiffres de signalement ne cessaient d'augmenter, qui justifiaient à eux seuls l'existence de la Centrale d'enregistrement[8]; cependant on savait que ce n'était que la pointe de l'iceberg et qu'un autre instrument d'enquête était probablement nécessaire pour connaître l'ampleur de cette délinquance.

En 1999, l'Office fédéral de la statistique avait commencé à élaborer un relevé sur la criminalité enregistrée par les autorités policières dans les cantons; devenu fonctionnel avec la publication de la statistique policière de la criminalité (SPC) en 2009, il n'intégrait pas d'items sur la cybercriminalité. Son intégration dans l'actuelle statistique policière de la criminalité n'a été achevée que récemment, les premières données, pour l'année 2020, étant publiées en 2021. La communication autour des résultats de la SPC de l'année 2020 a été largement focalisée sur la cybercriminalité. Cependant, les limites du relevé sont bien connues et explicitées par l'OFS lui-même.

En effet, les experts s'accordent sur le fait que le chiffre noir est – dans ce domaine – particulièrement élevé. Même si les enregistrements dans la SPC (24 000 infractions enregistrées) sont supérieurs aux signalements dans MELANI (10 700 annonces)[9], ils ne représentent pas la réalité du volume d'infractions commises dans le domaine de la cyberdélinquance, ce qui pose la question de l'adéquation du relevé avec le type de criminalité.

Ces analyses seraient plus valides si on disposait de données provenant d'enquêtes auprès de la population, des entreprises et des administrations, visant à évaluer le taux d'incidence et de prévalence de ces infractions, en combinaison avec les taux de dénonciation aux autorités de police (taux de reportabi-

8 MELANI est passé de quelques milliers de cas signalés, à plus de 10 000 cas récemment.

9 Dans son rapport semestriel 2020/1, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) indique qu'elle a reçu 5162 annonces de possibles infractions de type cybercriminalité, dont 3000 pour de « simples » escroqueries. Dans son rapport semestriel 2020/2, elle fait état de 5542 nouveaux cas, loin de l'explosion qui était attendue en raison de l'accroissement vertigineux de l'usage de l'internet, suite à la survenue de la pandémie COVID-19 en 2020.

lité). Il est certain que le taux de criminalité ainsi mesuré exploserait, tant sont nombreux les courriels de *fishing*[10], les messages de *pharming*[11] ou les abus et tentatives d'abus de cartes de crédit. A ce sujet, on peut renvoyer à des travaux ayant tenté, ces dernières années, d'évaluer le volume, la tendance et la nature des cybercrimes économiques, en particulier ceux de Michael Levi[12]. Ce dernier considère que si toutes les données permettent de penser à une croissance de cette forme de délinquance, sa croissance est bien inférieure à celle du volume des transactions sur internet, qu'il s'agisse du *shopping* en ligne, des actions de réservations ou toute autre activité devenue de routine. Il conclut son analyse (qui garde toute sa valeur cinq ans après sa publication) en se posant la question : « *What metrics are appropriate for judging the threat and harm from cybercrimes and their impact on national and human security* ? »[13].

4. La poursuite pénale – un empilement d'obstacles

En l'absence de données un tant soit peu complètes et cohérentes permettant d'évaluer de manière générale le volume et l'évolution de la cybercriminalité, il faut aborder à ce stade la question des problèmes de la poursuite pénale.

On constate tout d'abord qu'on ne sait pas grand-chose sur l'enregistrement des plaintes par les autorités de police, les raisons et les mobiles des personnes ou des institutions lésées qui déposent plainte et le traitement de ces plaintes. Aussi, peu a été rapporté sur les efforts faits ces dernières années par les autorités policières des cantons pour former l'ensemble de leurs agents au traitement des plaintes concernant des cyberdélits ; rien n'a encore été étudié en matière de formation plus poussée des agents devant réaliser, voire conduire les enquêtes policières, établir les preuves d'un type nouveau et préparer les dossiers à remettre aux autorités de poursuite pénale.

Les difficultés de la poursuite pénale en matière de cybercriminalité se situent sur trois niveaux.

Sur le plan technique, tout d'abord :

- Les délinquants ont toujours une longueur d'avance, étant donné que les autorités de poursuite pénale sont essentiellement réactives, même si elles tentent de réaliser aussi des actions prospectives ;

10 Appelé « hameçonnage » en français, le *fishing* consiste à se faire passer pour une organisation légtime pour obtenir des données personnelles ou des accès à des comptes.

11 Le *pharming*, « dévoiement » en français, vise à dérouter le traffic web – notamment d'institutions financières – vers un site sous contrôle de cyberdélinquants.

12 Michael Levi, Assessing the trends, scale and nature of economic cybercrimes : overview and issues, in : Crime, Law and Social Change, vol. 67, 2017, 3 ss.

13 *Idem*, 3.

- Les agents de police et les procureurs doivent avant tout comprendre les phénomènes et les modes d'action des auteurs d'infractions, avec une diversité croissante d'actions entreprises, du *fishing* au *pharming*, d'une attaque par déni de service (les DoS) au *Darknet*, parmi d'autres ;
- Un autre problème technique consiste dans la conservation des traces numériques, sur le plan des activités localisables dans les ordinateurs en Suisse, mais également concernant les adresses IP ;
- La poursuite pénale doit également faire face aux multiples procédés d'anonymisation utilisés par les auteurs d'infractions, qu'il s'agisse d'usurpation d'identité (« *spoofing* »), de l'usage de réseaux privés virtuels (VPN) ou du réseau TOR, ou de mails auto-détruisants ;
- Pour compliquer les choses, il faut encore ajouter à cette liste les difficultés d'accès au contenu des échanges effectués par l'intermédiaire de messageries cryptées (WhatsApp, Signal, Skype, etc.).

Ensuite, sur le plan juridique avec, à titre d'exemples :

- L'absence de définitions harmonisées et incontestées pour désigner les infractions à poursuivre, mais surtout pour lesquelles une entraide judiciaire internationale est souhaitable ;
- Des incertitudes quant aux qualifications des infractions, en raison de la complexification des affaires, des modes opératoires et de l'implication d'un nombre croissant d'acteurs aux rôles fort divers ;
- La difficulté d'identification du ou des lieux de commission de l'infraction, voire la multiplicité des lieux de commission des infractions, notamment quand elles sont commises depuis l'étranger ;
- Le manque d'entraide judiciaire internationale réglée en matière de cybercriminalité. Même si les conventions d'entraide en matière de poursuite pénale des cyberdélinquants se multiplient, la coopération internationale est encore souvent très lente, bureaucratique et loin de l'efficacité que demanderait une action concertée.

Enfin, sur le plan de la compétence en matière de poursuite pénale, en présence d'au moins deux intervenants possibles, à savoir :

- Le Ministère public de la Confédération quand une infraction est commise par des auteurs principaux situés à l'étranger impliquant – potentiellement – un crime organisé ou de la criminalité économique commise depuis l'étranger ou impliquant plusieurs cantons (art. 24 al. 1 CPP) ;
- Les ministères publics des cantons quand il s'agit, par exemple, de poursuivre des « *money mules* », soit des personnes domiciliées en Suisse et se mettant à la disposition de personnes situées à l'étranger pour réaliser des

transactions bancaires en vue du blanchiment de fonds obtenus par le biais d'infractions de type cyberdélinquance.

Une fois additionnés, ces facteurs ralentissent l'action de poursuite pénale, voire la rendent impossible. C'est notamment le cas lorsque la majorité des traces ont disparu ou n'ont pas été correctement conservées, voire ne peuvent être reconstituées, ou encore quand les auteurs d'infractions ont fermé des sites, des comptes, des enseignes ou des entreprises en changeant également, entre temps, de pays de résidence et d'action ; ces changements nécessitent alors de nouvelles démarches d'entraide judiciaire auprès d'Etats, dont l'autorité judiciaire ne se montre pas forcément coopérative.

Cette situation a conduit les Etats à développer des stratégies nationales de protection contre les cyberrisques (National Cyber Security – NCS). La Suisse a formulé sa première stratégie pour la période de 2012-2017. La seconde, plus importante et englobante, couvre la période 2018-2022 et contient « un cadre stratégique pour améliorer la prévention, l'identification précoce, la réponse et la résilience dans tous les domaines relevant des cyberrisques »[14]. Sa vision doit être réalisée à travers sept objectifs stratégiques qui ne font pas référence, faut-il le souligner, à la poursuite pénale. En revanche, parmi les 12 sphères d'action et mesures à prendre, on trouve la poursuite pénale, avec quatre mesures à développer :

- Une analyse générale de la situation de la cybercriminalité[15] ;
- Un réseau de soutien à la conduite des enquêtes des autorités de poursuite ;
- La formation ;
- Un office central du cybercrime[16].

Dans la description de la situation initiale, le document retient que l'ensemble des domaines retenus doit être fortement développé.

Depuis, diverses avancées ont été réalisées. Le nouveau Centre national pour la cybersécurité (National Cyber Security Center – NCSC) fait un bilan globalement positif de l'atteinte partielle de la première mesure mentionnée ci-dessus, à savoir l'analyse générale de la situation, en mentionnant des tests avec un logiciel d'enregistrement et d'analyse forensiques des cas (au nom de PICSEL), ainsi qu'un instrument d'harmonisation de language (Cyber-CASE).

14 The Federal Council, National strategy for the protection of Switzerland against cyberrisks (NCS), 2018-2022, document daté d'avril 2018 (selon notre traduction).

15 Le texte cité ci-dessus (n. 14) parle d'abord de « *picture of the cybercrime situation* » (10), ailleurs de « *national case overview* » puis de « *national real-time picture of the cybercrime situation for policing purposes* » (21).

16 18. Picture of the cybercrime situation ; 19. Investigation Support Network for Digital Law Enforcement ; 20. Training ; 21. Central Office for Cybercrime (la traduction de ces termes dans le texte est de l'auteur) in : FITSU, National Strategy for the protection of Switzerland against cyber risks (NCS), 2018-2022, Berne, daté d'avril 2018.

Cependant, on peut penser qu'on est encore loin de disposer d'une image en temps réel de la situation du cybercrime à des fins d'action policière et de poursuite, notamment en raison de l'absence de progrès en matière de l'établissement d'un réseau de soutien aux enquêtes sur la cybercriminalité. Etant donné que ces deux mesures doivent être réalisées en coordination avec le projet d'Harmonisation de l'informatique policière suisse, il faudra probablement encore un peu de temps avant de disposer du nouvel environnement nécessaire à une action efficace en matière de poursuite pénale.

En ce qui concerne la troisième mesure, à savoir la formation relative au traitement des plaintes, voire des affaires de cybercrime, une brève instruction en ligne a été dispensée aux agents des corps de police des cantons. D'autres actions de formation plus avancées, spécifiquement pour les cadres de police et les procureurs, sont prévues. En ce qui concerne la quatrième mesure, un nouvel office central du cybercrime est effectivement devenu opérationnel en juillet 2020 (mais sa dénomination n'est pas encore uniforme).

5. Les réaménagements institutionnels

Il est impossible, dans cette brève contribution, de retracer les développements institutionnels qui ont précédé la mise en œuvre en 2018 du Centre national de compétence pour la cybersécurité au sein du Département fédéral des finances. Alors qu'il s'agissait initialement d'une activité définie principalement comme policière, institutionnellement rattachée à l'Office fédéral de la police, la cybersécurité est devenue une tâche transversale impliquant un grand nombre d'acteurs de l'Etat, de l'économie et des hautes écoles, y compris trois départements fédéraux et ses conseillers. On peut affirmer que la gestion des cyberrisques est devenue, avant tout, autre chose qu'une action pénale, l'objectif premier étant moins de poursuivre des personnes que de garantir la prévention, la gestion de crise et la résilience en cas de survenue de cyberattaques. Si les bases ont été posées dès mi-2018, avec les décisions sur les grandes orientations de l'organisation de la Confédération en matière de cyberrisques, c'est en réalité à partir du 1er juillet 2020 que la nouvelle organisation a été considérée comme légalement fondée et opérationnelle[17].

17 Voir notamment : Rapport du Conseil fédéral du 27.11.2019 sur l'organisation de la Confédération pour la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques. Egalement : Communiqué du Conseil fédéral du 31.1.2019 : Le Conseil fédéral donne le coup d'envoi à la création du Centre de compétences pour la cybersécurité ; ainsi que celui du 28.5.2021 : Protection contre les cyberrisques : le Conseil fédéral adopte une ordonnance et une augmentation des effectifs.

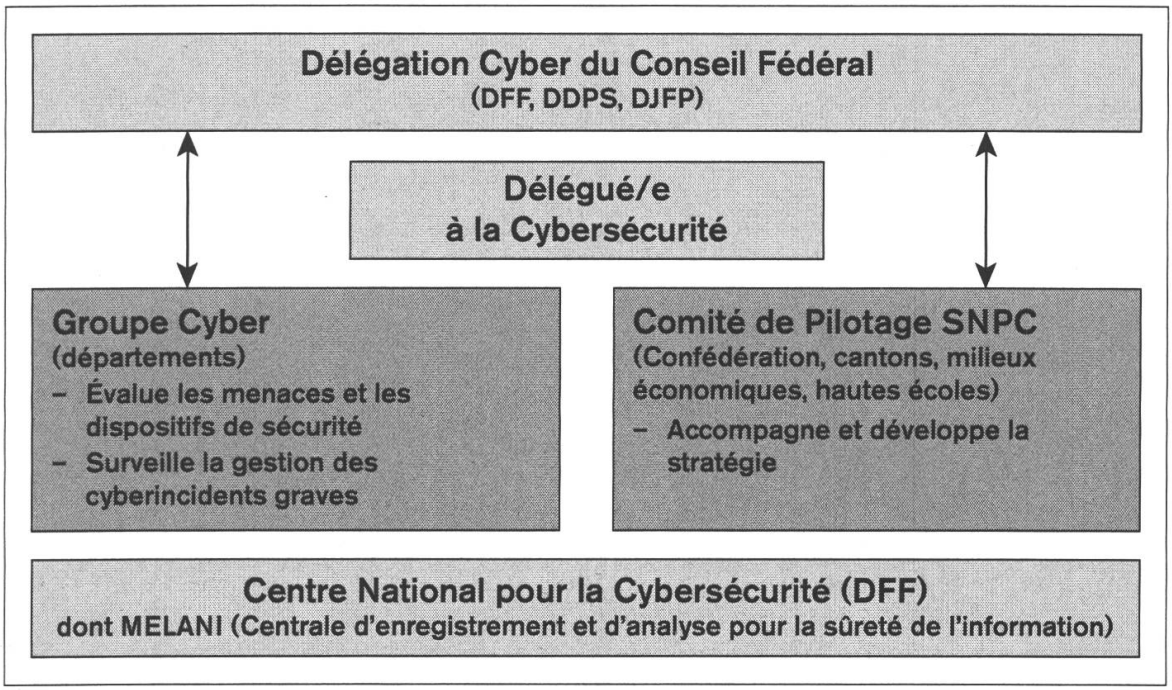

Figure 1 Organisation de la Confédération dans le domaine des cyberrisques, présentée dans le rapport cité dans la note de bas de page 17.

Cette nouvelle organisation est d'abord constituée d'une « Délégation cyber » du Conseil fédéral, composée des trois conseillers fédéraux concernés – à savoir ceux des départements des finances, de la défense et de la justice et police – qui ont la tâche de superviser la définition et la mise en œuvre de la stratégie nationale en matière de cybersécurité. Associé au Département fédéral des finances et directement sous son autorité, le délégué à la cybersécurité assure la direction stratégique de la cybersécurité de la Confédération. Le Groupe Cyber interdépartemental est, quant à lui, censé renforcer la coordination entre les trois domaines de la sécurité, de la défense et de la poursuite pénale. Le Comité de pilotage SNPC doit, lui, garantir la mise en œuvre cohérente de la stratégie et son développement futur, en impliquant un nombre plus important d'intervenants dans le domaine. Enfin, le centre de compétence lui-même est doté, en sus du secrétariat du délégué, d'un pool d'experts sur la standardisation et la régulation de la sécurité informatique ainsi que d'un groupe de techniciens en matière de sécurité de l'information de la Confédération.

Du côté de la poursuite pénale, il existe un consensus quant au besoin d'une coopération plus étroite entre autorités de police et de poursuite pénale, entre cantons et Confédération et entre unités d'analyse et celles en charge des opérations. De ce fait, le NCSC travaille à la définition d'« une méthode de travail nationale destinée au transfert de savoir et à la coordination stratégique et

opérationnelle en matière de lutte contre le cybercrime »[18]. S'il s'agit peut-être d'une méthode, on peut surtout parler d'un organigramme, d'une plateforme, dénommée « Cyberboard » en franglais, composée d'un organe de pilotage stratégique (Cyber-Strat) et d'un domaine opérationnel, lui-même constitué de diverses unités, dont la Centrale d'enregistrement MELANI et autres centres de coordination et d'échange. Ensemble, ces unités visent à favoriser la production d'une vue d'ensemble des infractions commises ou des affaires en cours (Cyber-CASE), d'une part, et d'une évaluation de l'état ou d'un tableau de la situation (Cyber-STATE) d'autre part. Dans leur évaluation produite en octobre 2020, le NCSC affirmait, de façon un peu optimiste, que « [l]es autorités de poursuite pénale disposent donc de bases adéquates pour développer régulièrement les capacités de lutte contre le cybercrime au sens d'une tâche commune et mettre en œuvre les mesures de la SNPC »[19].

Cette vision des progrès accomplis doit être tempérée, si l'on se réfère à la prise de position de Dunn Cavelty et Florian Egloff[20]. En effet, ces deux cyberexperts de l'EPFZ se demandent si l'on peut considérer que les tiraillements entre les sphères de responsabilité ont été résolus ou si l'on continue à poursuivre des solutions typiquement suisses, décentralisées et nécessitant une « coordination massive ». Ils considèrent qu'il s'agit bien d'un pas dans la bonne direction, mais que les arrangements organisationnels ne suffisent pas à assurer la cybersécurité du pays. Des négociations complexes et dynamiques devront être menées, d'abord entre Etat et économie, puis entre Etat et citoyens et enfin entre citoyens et économie. Dans tous ces domaines, des conflits d'objectifs existent – entre mesures pour la sécurité des systèmes d'information et droits des citoyens ou encore entre surveillance généralisée et liberté des acteurs économiques, pour ne citer que ces exemples. Finalement, il s'agit de savoir comment l'Etat remplit son rôle de garant d'une technologie sûre pour la société et l'économie, sans empiéter plus que nécessaire sur les droits des acteurs économiques et des citoyens. Tout semble indiquer que cette tâche s'effectue de moins en moins sur le terrain de la poursuite pénale.

18 NCSC, Rapport sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022, daté d'octobre 2020, 22.

19 *Idem*, 22.

20 Myriam Dunn Cavelty/Florian J. Egloff, Switzerland's new cyberscurity centre is a step in the right direction, opinion Swissinfo.ch, September 7, 2020, accessible sous ‹https://www.swissinfo.ch›.

6. Conclusion

Au travers de ce survol de l'évolution de la cybercriminalité et de la réponse apportée face à ce phénomène, il s'agissait de montrer qu'il existe une nécessité – voire une urgence – pour les criminologues de se saisir de cette nouvelle problématique. Elle n'est pas seulement l'affaire des chercheurs impliqués dans la réponse informatique, juridique ou pénale à la cybercriminalité, mais aussi un domaine dont les criminologues doivent se saisir[21]. L'étude criminologique de ce phénomène n'en est en effet qu'à ses débuts, qu'il s'agisse aussi bien du volume, de la structure ou de l'évolution de cette criminalité, analysée en comparaison avec les formes plus traditionnelles de la délinquance, que de son impact sur les activités de la police et des autorités de poursuite pénale, ou encore des dommages causés à la société, à l'économie ou à l'Etat – autant de questions qui méritent l'attention.

21 Brandon Valeriano/Miguel Aberto Gomez, The Failure of Academic Progress in Cybersecurity, in : Guest Blogger for Net Politics, Council of Foreign Relations, July 20, 2020, (consulté le 1.6.2021). Ces auteurs considèrent que le domaine des *cybersecurity studies* présente un déficit de méthodologies spécifiques et de réflexions épistémologiques, que la collecte de données est insuffisamment fondée et que ce domaine doit encore être fortement développé en tant que discipline académique. Au vu du nombre croissant d'articles publiés dans des revues évaluées par des pairs et des forums d'échanges scientifiques établis, ils demeurent néanmoins optimistes.