La criminalité 2.0, une menace invisible pour Haïti

Par James Boyard

La criminalité traditionnelle, tels, les assassinats, le kidnapping, le vol à main armée, le trafic illicite de drogue (…) ont tous en commun le fait d'être sujets d'une publicité quotidienne, intense et profondément illustrative tant dans les médias traditionnels que sur les réseaux sociaux. Pourtant, à côté de ces crimes spectaculaires et surmédiatisés, notre société fait face à partir du courant de l'année 2010 à un nouveau type de criminalité plus discrète et plus immatérielle, baptisée élégamment par les experts de « Criminalité 2.0 », ou de manière plus commune de « Criminalité cybernétique ».

En effet, depuis l'introduction des nouvelles technologies de l'information et de la communication (NTIC) au début des années 1990, divers secteurs de l'économie et de l'administration publique haïtienne se sont progressivement et largement informatisés, afin de devenir plus performant ou plus compétitifs. Mais, le hic est que l'institutionnalisation accélérée des outils télématiques ou cybernétiques n'a pas seulement le mérite de favoriser une meilleure gouvernance de l'ensemble des activités sociétales, elle a aussi malheureusement le tort d'exposer certains domaines sensibles de la vie publique ou de la vie privée à des interférences d'individus dangereux ou malhonnêtes. Ce sont justement ceux-là qu'on appellera les « cybercriminels ».

Notre objectif ici est non seulement d'appeler l'attention de l'opinion publique nationale sur l'existence de ces « cyber-menaces » qui commencent discrètement à faire partie de l'univers de la criminalité transnationale organisée en Haïti, mais aussi d'offrir une meilleure conceptualisation et compréhension des enjeux et défis liés à ces nouvelles menaces de sécurité dans le monde, et plus particulièrement dans la société consumériste haïtienne.

Au final, nous espérons bien entendu que les législateurs, les politiques, les citoyens et les entreprises, notamment les banques prendront toute la mesure du problème et accepteront en conséquence de donner écho aux stratégies de défense, de prévention et de répression que nous proposons pour faire face à ces nouvelles menaces de sécurité.

A.- Les caractéristiques de la criminalité cybernétique

Quel que soit leur dénomination particulière, crime cybernétique, cyber-menace, cyber-attaque, cyber-incident, cybercriminalité, cyber-crime, crime virtuel, cyber-délinquance, crime informatique ou délinquance 2.0, ce nouveau champ de la criminalité désigne toutes les formes de délit ou de crime commis en ligne, via des réseaux de communication ou des systèmes d'information électronique, par un individu ou un groupe d'individu, travaillant pour son compte ou le compte d'une organisation ou d'un gouvernement. Par extension, la criminalité cybernétique intègre aussi toute forme de malveillance, d'escroqueries, de fraudes, d'extorsions, d'abus, d'espionnage, d'harcèlement effectuée au moyen d'outils téléphoniques, cartes à puce, etc.

Même si le champ d'action de la cybercriminalité est trop vaste pour en délimiter les contours, il convient en général d'y regrouper les principaux crimes et délits suivants :

- Les usurpations d'identité commis par le truchement de l'internet, aux fins de d'escroquerie ou d'atteinte à la réputation de la victime ;
- L'hameçonnage ou « phishing », permettant à des individus de voler des mots de passe via de faux comptes bancaires afin de perpétrer des vols ou de l'escroquerie ;
- Les attaques à l'aide de spams, de logiciels malveillants ou de logiciels programmés pour tirer parti des failles du système informatique d'une institution et créer des bugs informatiques considérables ;
- Les tentatives de piratage informatique afin de voler des éléments de propriété intellectuelle ou des informations confidentielles appartenant à des entreprises ou des gouvernements ;
- Le ciblage d'actifs d'importance nationale, d'intérêt stratégique ou économique, tels que les réseaux électriques, les réseaux de transport routier, ferroviaire ou aérien ;
- Le cyber-harcèlement sexuel et la cyber-pédophilie ;
- La publication illégale de photos ou d'images intimes ou de Sextape dans le but de nuire à la réputation d'un individu ou de se venger ;
- Les Montages malicieux d'images ou de sons d'une célébrité ou d'un simple individu dans un contexte inapproprié ;

- La Diffusion ou partage de contenu pénible, tels des photos ou vidéos d'actes d'une extrême violence ou des documents prônant la violence, la haine ou des actes terroristes envers un individu, une catégorie sociale, une institution ou un gouvernement (…).

Quoi qu'il en soit, dépendamment de la motivation des cybercriminels, il convient aussi d'en distinguer trois catégories :

- ***Les Hackers :*** motivés par un complexe de la performance ou le souci du jeu ou de se mesurer et qui cherchent à pirater certains systèmes informatiques plus par défi que par un intérêt de nuire ou de s'enrichir ;
- ***Les Crackers :*** inspirés par des intérêts idéologiques et qui tentent d'abimer ou de supprimer les informations électroniques de certaines institutions dans le but de les ruiner ou les handicaper ;
- ***Les Fraudeurs :*** motivés par des intérêts économiques et qui emploient les fraudes informatiques simplement comme moyen supplémentaire pour obtenir des gains financiers illicites ;
- ***Les cyberactivistes :*** qui sont des militants d'une cause ou des adeptes d'une idéologie extrémiste, mettant à profit leur compétence en piratage informatique dans le but de promouvoir leur cause ou provoquer des changements politiques ou sociétaux.

Tout ceci pour dire qu'il n'existe pas un « idéaltype » de cybercriminel, ni de pays ou de secteurs de la société qui ne soient pas exposés à la délinquance, aux opérations criminelles ou aux actions terroristes, via, le cyberespace, par le truchement des nouvelles interfaces d'exploitation, tels que, Facebook, Twitter, Myspace, Google, Flickr, LinkedIn,Whatsapp, TicToc (…)

En effet, ces nouveaux vecteurs de recherche ou de support informationnel, datant pour la plupart du milieu des années 2000 ont par rapport à l'ancienne version d'internet alimentée par Altavista, Napster, Netscape, Yahoo (…), un ensemble de nouvelles particularités techniques et médiatiques qui suscitent à la fois un attrait plus fort chez les utilisateurs individuels et institutionnels et, par conséquent, une convoitise plus grande de la part du milieu criminel et clandestin.

Pour preuve, par opposition à l'internet de la première génération, celui de la deuxième génération, communément appelé « Web 2.0 » est caractérisé par au moins trois attributs techniques susceptibles d'être exploités par les esprits enclins à la transgression des lois ou des règles d'éthiques :

- ***La Décentralisation :*** La capacité de l'internet à s'étendre sans aucune frontière dans toutes les régions et tous les milieux sociaux, rend son usage accessible à presque tout le monde. Cette démocratisation d'accès à l'internet permet non seulement l'émergence de groupes criminels spécialisés, mais aussi et surtout la constitution et la multiplication des cas de délinquance isolés ;

- ***L'Interactivité :*** La possibilité d'accroissement des interactions sociales sur le web a aménagé un espace de plus en plus grand pour l'affirmation d'un « moi » distant et anonyme, multipliant l'usage des « pseudos » pour participer à la « co-construction » de la communauté sociale du Web. Ce sentiment d'anonymat et d'éloignement de ce « moi » par rapport aux activités opérées sur la toile, incite certaines personnes à violer toute sorte d'interdits, tout en espérant échapper aux conséquences de droit ;

- ***La Connectivité :*** L'interconnexion croissante des entreprises, notamment les banques, au réseau mondial est devenue non seulement une nécessité fonctionnelle, mais aussi une norme standard en matière de gouvernance financière. Cependant, l'interconnexion n'a pas seulement l'avantage de faciliter les échanges entre les banques et entre celles-ci et leurs clients, elle a aussi la faiblesse d'exposer les données bancaires à des risques constants de destruction ou de détournement criminel.

Dans ce contexte de développement du cyberspace ou les cyber-attaques sont devenues les méthodes privilégiées des criminels en quête de gains illégaux, le cout mondial de la cybercriminalité est estimé chaque année entre 375 à 575 milliards de dollars, soit 100 milliards de dollars uniquement pour les infractions visant les Etats-Unis.

B.- Les cas de crime cybernétique auxquels sont exposés Haïti

Puisque le cybercriminel a nécessairement besoin d'utiliser le support informatique ou internet pour réaliser ses activités illicites, il n'étonne point que les pays les plus exposés à cette criminalité cybernétique soient précisément ceux-là qui bénéficient d'un haut niveau d'interconnexion en matière d'internet. Cependant, même si en Haïti, le niveau d'interconnexion et d'utilisation d'internet est encore très modérée ou disons mieux, le plus faible de la région, notre pays commence malheureusement aussi à expérimenter certains aspects de la criminalité cybernétique, dont :

- ***Les vols dans les distributeurs automatiques de billets (ATM), via de fausses cartes électroniques :*** Quoi que la plupart de ces faits n'aient pas été ébruités exprès afin de préserver la crédibilité et l'image publique des institutions bancaires victimes, quelques Banques haïtiennes ont plusieurs fois été la cible de ce genre de vols sophistiqués. La particularité de ce crime c'est qu'il met presque toujours en scène des ressortissants de certains pays de l'Europe de l'Est ou Centrale, notamment des Roumains qui ont fait le voyage en Haïti spécialement pour réaliser leur forfait. Aussi, pour s'assurer de prélever le plus d'argent possible, ces criminels informatiques s'empressent-ils de faire des virées dans plusieurs départements du pays largement desservis par le système ATM ;

- ***Le sabotage ou la destruction de sites informatiques d'institutions privées ou publiques :*** plusieurs institutions publiques ou privées, notamment universitaires et commerciales ont du faire face à des actes de sabotage sur leur site web officiel, le plus souvent perpétrés par des éléments externes à l'institution ou des anciens employés du service informatique qui ont récemment été mis à pieds. Ces institutions ont été parfois obligées de faire appel à des experts haïtiens ou étrangers chèrement payés pour rétablir l'intégrité de leur site ou construire un nouveau site internet mieux sécurisé ;

- ***Le détournement des données multimédia (photos, vidéos ou voix) à des fins de désinformations*** : il s'agit de l'un des crimes informatiques le plus communs en Haïti, du fait qu'ils impliquent en général des délinquants plus ou moins jeunes ou des activistes politiques, n'ayant que peu de compétence dans l'utilisation des

nouvelles technologies de l'information et de télécommunication. Ils agissent parfois pour leur propre compte, mais aussi souvent pour le compte d'une autorité politique ou administrative ou d'un groupuscule politique. Leurs cibles sont en général des personnalités politiques ou des hauts fonctionnaires de l'Etat dont ils manipulent les photos, vidéos ou enregistrements sonores sur Facebook, Whasapp ou Youtube afin d'attenter à leur image publique ou les mettre dans une situation embarrassante ;

- ***Le vol ou l'interception des données informatiques ou des données de téléphones portables afin de violer le droit à l'intimité ou de procéder à des chantages*** : ce type de criminalité est aussi baptisé de « cybercrime passionnel » ou de « Vendetta amoureuse » dans la mesure où il est en principe motivé par la vengeance suite à une rupture amoureuse non assumée par l'un des partenaires. Il se manifeste souvent par la menace de rendre public le contenu embarrassant du téléphone au cas où la victime n'exécuterait pas la volonté de l'ex-partenaire ou du délinquant. Quoi que ce type de crime touche toutes les catégories sociales en Haïti, les statistiques des plaintes ou des dénonciations parentales ont révélé que ce sont surtout de jeunes écolières ou de jeunes filles insouciantes qui en sont le plus souvent victimes. Au demeurant, les séquelles psychologiques néfastes que ces genres de cyber-incidents imprègnent sur les jeunes victimes méritent à elles seules qu'on s'y attarde ;

- ***L'utilisation des réseaux sociaux aux fins de propagande illicite, d'appel à la haine ou à la violence :*** avec l'aggravation et la radicalisation de la crise politique haïtienne, cette sous-catégorie de cybercrime, proche du « terrorisme publicitaire » est en augmentation exponentielle, au point que certains réseaux comme Facebook, Youtube ou Whatsapp sont devenus aujourd'hui en Haïti le plus grand espace pour manipuler l'opinion publique, endoctriner des groupes sociaux-cibles ou diffuser des rumeurs. En effet, presque tous les jours des groupes d'activistes à visière découverte ou cachés derrière des noms d'emprunt ou des pseudonymes donnent largement écho à des menaces d'agression contre d'autres groupes politiques ou sociaux. Cette rhétorique de guerre verbale qui prend pour scène les réseaux sociaux, dont principalement Facebook, Watsapp, Youtube a le plus souvent pour

toile de fond, la promotion de la lutte des classes, de la haine raciale ou de la violence politique ;

- ***L'interception et la diffusion sur internet ou les réseaux sociaux des documents confidentiels*** : la crise politique haïtienne prend de plus en plus la forme d'une guerre totale entre les principaux protagonistes où tous les coups sont bons pour atteindre ou vaincre l'adversaire. Dans cette ambiance de faillite de l'éthique publique et politique, la chasse aux documents confidentiels dans les institutions publiques aux fins de leur diffusion dans les réseaux sociaux est devenue une grande priorité pour certains groupes de militants ou d'activistes s'érigeant en lanceurs d'alerte. En général, ces criminels du Web ciblent des documents sensibles, tels, des notes de service restreintes, des copies de chèques, des notes de renseignements, etc., qu'ils présentent sur les réseaux sociaux comme des documents compromettant, afin d'embarrasser l'Etat, l'auteur ou le destinataire de tels documents. La Présidence, la Primature, la PNH et plusieurs ministères dont celui de l'Intérieur et des collectivités territoriales et celui de l'Economie et des finances ont été plusieurs fois victimes de ces cyber-délinquance ;

- ***L'utilisation de certains sites d'internet, de compte WhatsApp ou du système « Mon Cash » à des fins d'escroquerie*** : avec l'introduction du système de transfert d'argent online, popularisé par le support téléphonique, de jeunes délinquants du Web s'associent en bande organisée pour escroquer les citoyens via le système d'application « Mon Cash ». Par cette pratique d'«hameçonnage » ou « phishing », ces criminels du Web arrivent certaines fois à cloner le système mon cash afin d'intercepter les transferts d'argent ou à monter de fausses agences de distribution online leur permettant d'accéder à des transferts d'argent ou des numéros de carte de crédit de clients naïfs, pensant avoir passé leurs commandes auprès d'une agence commerciale crédible. Cette forme d'escroquerie est réalisée aussi par des cybercriminels étrangers souvent localisés en Afrique qui arrivent à prendre possession des contacts de votre adresse courriel afin de solliciter à ces derniers de l'aide financière en votre nom ;

- ***La Création de faux compte d'internet (Facebook, Twitter, etc) au nom de certaines personnalités*** : il s'agit là d'une autre pratique de cybercriminalité très

en vogue en Haïti, motivée surtout par la vengeance ou le gain illicite. En effet, des délinquants restés dans l'ombre de leur ordinateur s'amusent à multiplier les faux comptes de certaines personnalités officielles ou médiatiques sur Facebook ou Twitter, dans l'objectif de diffuser de fausses informations émanant soi-disant de ces sources officielles ou d'escroquer des citoyens en se faisant passer pour ces personnalités politiques ou administratives, en leur promettant notamment des bourses d'études a l'étranger, des voyage à l'étranger ou un boulot dans une institution publique ou privée haïtienne La particularité de ce type de cybercriminalité c'est qu'elle peut affecter l'authenticité mêmes des sites ou comptes d'internet officiels en minant la confiance du public dans ces « Open sources ». La DCPJ regorge les cas de plaintes d'officiels de l'Etat ou de personnalités de la société civile victime de ces genres d'arnaque, dont des parlementaires, des Directeurs généraux de la PNH, des Ministres, des journalistes connus, etc. Le Premier ministre et le Président de la République eux-mêmes ne sont pas épargnés par ce genre de cybercrime ;

- ***L'Usurpation d'identité numérique :*** il s'agit d'une intrusion frauduleuse du cyber-délinquant dans l'ordinateur ou le compte de quel qu'un, dont il a usurpé au préalable les identifiants (mots de passe et nom d'utilisateur) afin de l'espionner ou collecter ses informations confidentielles. Même si, la plupart des cas d'usurpation d'identité numérique connus en Haïti n'impliquent que des proches (couples, groupes d'amis), plusieurs plaintes enregistrées par la PNH ont concerné aussi des collègues de bureau malhonnêtes, des individus verser dans le voyeurisme ou mêmes des fraudeurs inconnus ;

- ***La « Rançongiciel » ou « Ransomware » :*** agissant comme des programmes informatiques malveillants, la « Rançongicel », consiste à pénétrer illégalement à distance dans l'ordinateur d'un autre individu via un virus incrusté dans un mail contenant des pièces jointes ou des liens piégés, pour en chiffrer ses données et exiger ensuite à leur propriétaire une rançon ou d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer. Ce type de cyberdélinquance qui a été très active dans certains pays d'Afrique et d'Amérique latine commence à faire timidement son apparition sur le territoire haïtien, avec la numérisation de plus en plus de certaines Petites et Moyennes Entreprises (PME) ;

- ***Le cyber-rançonnage :***depuis tantôt cinq ans, certains individus se sont spécialisés dans les pratiques de chantages téléphoniques, consistant à appeler leur victime au téléphone pour les informer d'abord du fait qu'ils ont été payés par une tierce personne pour les kidnapper ou les assassiner, mais qu'ils seraient prêts à ne pas exécuter ce contrat, moyennant que la cible leur verse une certaine somme. Evidemment, tous les cas qui ont été signalés à la Police et qui ont fait l'objet d'une investigation au niveau de la DCPJ se sont révélés être que des tentatives de chantages de petits délinquants qui ont pu s'informer au préalable de l'identité et du numéro de téléphone de la victime soit auprès de complices faisant partie de ses personnels domestiques soit à partir des endroits habituellement fréquentés par celle-ci, comme les salons de beauté, les clubs de sport, etc. Il est arrivé même plusieurs fois que le maître chanteur qui se trouve à l'autre bout du fil appelle sa victime à partir de sa cellule au Pénitentiel national ;

- ***Les attaques par « déni de service », appelé encore en anglais the « Denial of Service attack (DoS)» :*** le procédé consiste à créer une rupture virtuelle ou artificielle d'un stock de produits vendu sur un site internet, en passant de grandes commandes dont le paiement sera différé ou en formulant de milliers de fausses requêtes, pour ensuite les annuler à la dernière minute. L'un des buts de cette attaque informatique par saturation en Haïti, c'est de rendre indisponible le produit ou le service afin de limiter le succès financier de celui-ci sur le site internet. Nous avons soupçonné des attaques de ce genre contre les titres de certains auteurs vendus en ligne sur le site internet de « Livres en folie 2020 ».

Bien entendu, d'aucuns peuvent toujours penser que les exemples de crimes cybernétiques que nous venons d'énumérer plus haut sont encore à un niveau très négligeable eut égard aux grandes attaques cybernétiques, voire aux risques de cyber-terrorisme aux quels certains Etats font déjà face. Mais, le problème est que l'indice d'accès numérique du pays risque d'évoluer qualitativement d'ici l'année 2030.

En effet, selon une étude du gouvernement haïtien, on évaluait déjà en 2006 le nombre d'abonnés aux opérateurs de téléphonie mobile à 3.7 millions, avec un investissement initial de la DIGICEL de 260 millions de dollars, nous pouvons penser aujourd'hui que le nombre d'abonnés ait été triplé. D'un autre côté, les utilisateurs d'internet ont été estimés en 2012 à

plus de 1.3 million, ce qui représentait déjà à l'époque 14% de la population. Or, pour promouvoir l'expansion de la connectivité et du maillage numérique du territoire, le gouvernement haïtien se propose de réaliser dans le cadre de l'exécution de son Plan stratégique de développement projetant Haïti au rang de pays émergeant d'ici 2030, les projets suivants :

- la remise en fonctionnement du câble sous-marin de BATELCO qui relie les Bahamas à Haïti et à Miami ;
- le raccordement à au moins un second câble sous-marin dans la Caraïbe pour assurer un circuit redondant avec le câble de BATELCO ;
- la construction de liens optiques terrestres internationaux entre Haïti et la République dominicaine ;
- la construction d'un réseau de 6000 kilomètres de câbles en fibre optique ;
- le déploiement de réseaux WiMAX dans les milieux isolés (…).

Fort de toutes ces grandes perspectives de développement en matière numérique, on peut légitiment penser que l'administration publique haïtienne, les entreprises commerciales, les banques et la majorité des citoyens haïtiens auront l'opportunité de bénéficier à court et à moyen terme d'une plus grande interconnexion à l'internet, ce qui risque bien entendu d'augmenter de manière exponentielle la vulnérabilité du pays face aux grandes menaces cybernétiques.

C.- Les moyens de lutte contre la cybercriminalité en Haïti : défis et perspectives

Même si les données de statistiques disponibles pour le moment en Haïti sur la criminalité cybernétique ne sont pas encore dans le rouge, à cause surement de ce déficit d'interconnexion du pays à l'internet de haut débit, de plus en plus d'institutions publiques ou privées haïtiennes s'activent pour faire un bond numérique dans les prochaines années, dans le but de devenir plus performantes et mieux intégrer les structures de l'économie mondiale. Dans cette perspective, conformément au Viel adage, « gouverner c'est prévoir », l'Etat haïtien a intérêt à agir de manière anticipative et proactive en mettant en place des outils législatifs, institutionnels et relationnels adaptés à ces nouvelles menaces afin de mieux les contenir.

Mais le hic est que, les seuls instruments de lutte dont dispose pour l'instant le gouvernement haïtien contre les menaces cybernétiques n'est qu'une simple cellule nouvellement créée au sein du Bureau des enquêtes spéciales de la DCPJ, dénommée justement « Cellule contre les crimes cybernétiques (CCCC) ». Cette unité composée de pas plus de cinq enquêteurs et informaticiens a la charge de mener sur tout le territoire la répression contre les crimes informatiques ou cybernétiques.

Or, comme c'est le cas ailleurs, même chez nos voisins dominicains, la lutte contre cette nouvelle forme de criminalité, pour être efficace et crédible, nécessite des efforts d'innovation institutionnelle ou d'ingénierie politique à trois niveaux complémentaires : législatif, technique et diplomatique.

(1) ***Du point de vue législatif :*** entant que nouvelles catégories d'infractions pénales, les crimes cybernétiques entrainent un triple défi pour les systèmes législatifs nationaux des Etats. Il s'agit d'un côté d'infractions dont la « qualification » est difficile à cause de leur nature virtuelle ou immatérielle. D'un autre côté, ils se réfèrent à des infractions dont l'« imputabilité » est difficile, du fait qu'il n'est pas toujours aisé de terminer les limites de la responsabilité. Est-ce l'individu ayant agi ou l'opérateur informatique, les fournisseurs d'internet ou les hébergeurs ayant la responsabilité de prévenir l'utilisation de leur outil télématique à des fins illicites ? Enfin, ces nouvelles catégories d'infractions pénales posent le problème de la « compétence juridictionnelle », en raison de leur difficulté de localisation.

En effet, vu qu'il peut s'agir souvent de crimes comportant un élément d'extranéité, comment donc déterminer la juridiction nationale ayant la compétence pour les réprimer. Est-ce la juridiction de l'Etat du territoire de la commission de ces crimes ? La juridiction de l'Etat du territoire de l'accessibilité des sites ? Ou la juridiction de l'Etat du territoire ayant subi les effets matériels de ces crimes ?

Quel que soit la politique législative qui sera privilégiée chez nous, le législateur haïtien se doit d'abord pour commencer par définir dans le Code pénal une nouvelle qualification juridique pour chaque catégorie et sous-catégorie de crimes cybernétiques, tels :

- le piratage informatique ;
- l'interception illégale de données numériques ;
- l'atteinte à l'intégrité des données ;
- l'atteinte à l'intégrité des systèmes (virus, spam et déni de service) ;
- la fraude informatique ;
- la falsification informatique ;
-les infractions se rapportant à la pornographie enfantine ;
-les infractions informatiques liées aux atteintes à la propriété intellectuelle et aux droits connexes, etc.

Ensuite, il convient pour le législateur d'établir de nouvelles échelles de peines adaptées à la dimension des préjudices commis, pouvant aller de simples sanctions pour délit mineur à de fortes condamnations criminelles.

Enfin, il serait indispensable pour le législateur de déterminer la compétence juridictionnelle des juges haïtiens dans une perspective résolument extraterritoriale, c'est-a-dire, allant au-delà de la conception traditionnelle de la « territorialité du droit pénal », du principe de la « compétence juridictionnelle en matière de droit commun » ou de la règle du droit des conflits de loi, dite « Lex loci delicti ».

Afin de limiter les cas de conflits de législation, cette extension extraterritoriale de la compétence du juge haïtien doit certainement être articulée autour du principe d'« Ubiquité », lequel permettrait de rattacher juridiquement un crime cybernétique même commis à l'étranger au territoire haïtien, dès lors que celui-ci y gênerait des préjudices ou des effets matériels substantiels.

(2) ***Du point de vue technique :*** par sa nature et ses effets, la criminalité cybernétique demeure un champ spécialisé du monde criminel. A ce titre, il serait trop facile de dire que les mécanismes de prévention et de répression de ces crimes doivent s'articuler prioritairement autour des experts ou des ingénieurs en informatique disposant des compétences techniques dans l'univers télématique pour détecter et localiser les sources des menaces cybernétiques. Pourtant, il n'en est rien.

Même si on ne doit pas reléguer au second plan l'importance de ces experts ou ingénieurs, la première ligne de front dans la lutte contre la criminalité cybernétique doit aussi être occupée par des juristes haïtiens spécialisés capables de déterminer avec aisance l'imputabilité de telle infraction, même lorsque celle-ci aura été détectée ou localisée par ces experts dans un pays étranger. Tout ceci, sans oublier le rôle des spécialistes en analyse multidimensionnelle et en intelligence économique qui interviendront plus pour anticiper les risques de cyber-attaques ou de cyber-agression.

En clair, au lieu de limiter la répression de la cybercriminalité à l'action de quelques enquêteurs et techniciens en informatiques regroupés au sein de la DCPJ, l'Etat haïtien aurait beaucoup à gagner à engager des moyens budgétaires nécessaires pour aider la PNH à constituer un forum hybride de spécialistes en lutte cybernétique ;

(3) ***Du point de vue diplomatique :*** étant pour la plupart des infractions pénales « désétatisé » et « déterritorialisé », la cybercriminalité échappe à la définition classique du territoire national et à la division traditionnelle entre les champs internes et externes de la sécurité. Dans ce contexte, aucun édifice technico-législatif institué en interne ne saurait intervenir seul dans la répression de ces catégories d'infractions sans le soutien d'autres Etats étrangers ou d'institutions internationales.

Fort de cet enjeu, le gouvernement haïtien se doit de s'investir diplomatiquement afin de développer une coopération internationale à la fois technique (fondée sur des échanges d'information ou de bonnes pratiques) et opérationnelle (mobilisant des juges et policiers haïtiens spécialisés dans le cadre d'enquêtes internationales conjointes). Cette coopération internationale est d'autant plus importante qu'elle permettrait à la justice haïtienne de résoudre ou prévenir les risques de conflits de législation ou de juridiction qui risqueraient de survenir dans les cas où le crime cybernétique comporterait un élément d'extranéité, sans oublier de résoudre les questions d'extradition d'auteurs de ces infractions pénales le cas échéant. Sur cette base, l'un des premiers efforts

diplomatiques à accomplir par le gouvernement haïtien dans ce sens serait de ratifier la Convention de Budapest du Ier juillet 2004 sur la cybercriminalité.