Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 4 Issue 2 (2024)

An Analytical Reading on the Repercussions and Harms of Cybercrime in the Age of Communication Technologies

Mohammed Elhadi Kaci *[1], Imane Hamri [2]

[1] University OF Akli Mohand Oulhadj Bouira- Algeria, 1000. (mo.kaci@univ-bouira.dz)

[2] University OF Akli Mohand Oulhadj Bouira- Algeria, 1000.(i.hamri@univ-bouira.dz)

Abstract

Through this study, we seek to identify the process and stages of development of electronic crime in relation to traditional crime, while explaining its most fundamental progress in light of the diffusion and growth of electronic crime technologies, communication and information and the rise of the Internet, as well as social networks in various spaces and vital areas.

This study presents itself as an analytical sociological reading to understand the dimensions of the phenomenon of cybercrime, the objective of which is to take into consideration the alarming figures and indicators which need to be elucidated.

Keywords : crime, cybercrime, communication technologies, misdeeds and computer crime, impact of cybercrime

Problematic

Introduction :

Ce qui distingue notre époque actuelle, c'est la révolution technologique massive qui a provoqué une vague de changements et de développements à tous les niveaux et en a été une porte d'entrée par laquelle l'humanité a obtenu de grands bénéfices et un changement qualitatif et historique dont le monde n'a jamais été témoin auparavant, en particulier dans le domaine de la science, des technologies de l'information, et d'Internet. Aujourd'hui, ces technologies ont créé de nouveaux comportements au niveau individuel et institutionnel, et ont contribué à l'émergence et à une dépendance quasi totale à l'égard de ces technologies qui ont envahi nos vies de manière inédite.

Problématique :

Le XXe siècle a été caractérisé par l'émergence de l'ère des technologies de l'information et de la communication et par d'énormes découvertes et inventions qui l'ont accompagnée au niveau scientifique et technologique, qui ont facilité l'émergence et la diffusion de l'utilisation des ordinateurs et le développement des réseaux d'information ; et de ce fait nous sommes témoins de la révolution du savoir et des nouvelles technologies, que l'on appelle le siècle de l'information, à savoir que les technologies de l'information et leurs outils se sont répandus à un rythme rapide, modifiant la vie des individus et des sociétés, et tous les segments de la société, aux niveaux individuel et institutionnel, et ont interagi de manière significative avec eux.

Beaucoup pensaient que nous étions en train de vivre des développements inhabituels avec la révolution du siècle, auquel s'ajouté de nombreux points positifs à notre vie quotidienne, et cela a produit de nouveaux modèles de comportement auxquels les gens n'étaient pas habitués, et beaucoup parmi nous pensent que toute invention humaine porteuse de progrès peut être aussi génératrice de comportements illicites. Parmi ces modèles répandus figurent la criminalité électronique et la délinquance informatique. Il y a aussi ceux qui croient que l'information ou le crime électronique sont le résultat de progrès rapides dans divers domaines scientifiques qui caractérisent notre époque actuelle, et ce que certains expliquent par une utilisation informatique significativement intensive à tous les niveaux.

Avec l'essor et l'ampleur de la cybercriminalité ces dernières années et la multiplicité de ses formes et de ses aspects, des voix se sont élevées ici et ailleurs pour tirer la sonnette d'alarme, alertant sur ses répercussions sur les plans économique, social, culturel et sécuritaire, d'autant plus qu'elle est considéré comme l'un des défis les plus dangereux auxquels l'homme moderne est confronté ; ce sont des crimes qui utilisent des outils très avancés et sont difficiles à prévoir.

L'importance de la problématique de cette intervention consiste de tenter à lever de l'ambiguïté et de mettre en lumière la cybercriminalité, compte tenu des grandes pertes matérielles et morales qu'elle engendre. Nous souhaitons également comprendre comment la cybercriminalité provoque des dommages économiques accrus dans le monde et des violations des droits de l'homme, notamment des dommages psychologiques et moraux aux personnes et aux institutions, et quels sont les défis auxquels nous pouvons faire face pour éliminer ces crimes, également de suggérer un ensemble de recommandations pour lutter contre la cybercriminalité et réduire ce phénomène qui s'amplifie avec ses graves dommages et répercussions ?

1/ **Notions de la cybercriminalité :**

Selon l'avis de plusieurs sources le terme cyberciminalité est un terme journalistique qui n'a toujours pas, dans la plupart des pays, de définition légale. Certes, il existe des différences et des similitudes dans les points de vue, d'opinions sur ce qu'est la cybercriminalité. Selon l'opinion de nombreux penseurs, l'origine de la cybercriminalité se compose de deux parties: cyber et crime; le terme est défini de manière très large par Schell et Martin pour qui, la criminalité inclut tous les crimes liés à la technologie, aux ordinateurs et à l'internet (Schell, B.H et C.Martin..2004).

Selon de nombreuses théories intellectuelles et scientifiques liées à cette question, plusieurs noms ont émergé, et à l'instar du terme cybercriminalité, nous entendons «crime d'information» ou « Cybercriminalité » car ils sont tous liés en rapport avec tout ce qui est cyberespace et l'information ; et souvent, selon un certain avis la typologie de cybercriminalité se distingue par les crimes commis par ordinateur ou commis avec tout type d'équipement numérique.

Avec l'émergence de l'informatique, et la croissance des aspects de la criminalité électronique, l'intérêt de nombreux chercheurs de diverses disciplines scientifiques s'est accru pour étudier et comprendre les dimensions du phénomène, ses risques, et suivre son augmentation et connaître ses effets négatifs. Plusieurs tentatives tentent de l'expliquer, certains l'abordent du point de vue technique, en soulignant que le crime d'information n'est rien d'autre qu'une activité criminelle dans laquelle la technologie informatique est utilisée directement ou indirectement comme moyen ou objectif pour commettre l'acte criminel envisagé et il est possible de l'éliminer, de le ralentir ou de le limiter simplement en arrêtant le fonctionnement de l'Internet mondial, en ralentissant sa vitesse ou en détruisant des sites. Agir selon cette conviction est une question extrêmement complexe, voire impossible, essayer de censurer internet reviendrait de vouloir censurer toutes les communications téléphoniques dans le monde… franchement personne ne pense que se

soit faisable (Liang.1999.p19), et chose qui ne peut être imaginée compte tenu de son importance et de ses avantages à tous les niveaux.

Quant aux partisans du courant juridique, ils estiment que donner une définition globale est une question difficile, contrairement à ce que pensent d'autres. Selon eux, définir les crimes électroniques nécessite de définir le vocabulaire nécessaire lié aux délits informatiques, qui sont l'ordinateur, le programme informatique, les données, la propriété, l'accès, les services et services vitaux. Et selon Don Porker, la criminalité informatique est : « toute acte illicite nécessitant une connaissance spécialisée de l'informatique, au stade de la perpétration, de l'enquête de police ou des poursuites pénales » (Parker.1985.P18).

Et sous l'angle de l'économie, certains d'entre eux considèrent que certaines personnes ont recours à ce comportement pour obtenir des gains, des moyens de subsistance et une porte d'entrée pour gagner de l'argent. Cela se conforme avec l'avis du juriste français « Masse Florant » qui considère que le cybercrime comme étant des attaques légales commises au moyen des technologies de l'information dans le but de réaliser un profit.

Parmi d'autres définitions, notamment celles liées au point de vue éthique, psychologique et sociologique; il y a ceux qui considèrent la cybercriminalité comme un comportement contraire aux contrôles et aux valeurs sociales et qui est illégal, voire immoral auquel l'individu ait recours pour commettre un crime en utilisant des outils techniques avancés de traitement et de transfert automatisés de données; ou toutes formes de comportements illégaux ou préjudiciables commis en utilisant des ordinateurs.

Selon notre analyse approfondie sur la question de l'évolution de la criminalité au fil du temps, de la criminalité traditionnelle à la criminalité électronique qui a balayé le monde, son aggravation et son expansion dans le temps et dans l'espace ont pris des dimensions sans précédent et en spectaculaire progression (Reverdy. 2005. P79), notamment au cours de la dernière décennie. Ces crime sont devenus une menace, et le phénomène des cybercrimes est préoccupant car il prend de l'ampleur et des conséquences adverses pour les individus, les industries, l'économie des gouvernements sont de plus en plus considérable et coûteux.

Quant à la définition adoptée par certaines organisations internationales sur la question du crime électronique, les Nations Unies en 2000, il s'agit d'un crime qui peut être commis au moyen d'un système informatique, d'un réseau informatique, au sein d'un système informatique, ou dans un environnement électronique ; et les experts de l'Organisation de Coopération et de Développement Economiques ont également défini la criminalité électronique :« tout comportement illégal ou contraire à l'éthique ou non autorisé, qui concerne un traitement automatique de données et/ou de transmissions de données » (Aterman et Bloch.1988.P530).

Ceci explique que l'humanité a été témoin du crime à travers les différentes périodes qu'a connu l'être humain, et son développement est lié à l'évolution du mode de vie dans divers espaces sociaux, et il variait en fonction de ses motivations et des circonstances sociales, et ainsi en fonction du temps et du lieu.

2/De la criminalité traditionnelle à la cybercriminalité :

Le crime est connu à travers les différentes périodes, et son développement est lié à l'évolution du mode de vie dans divers espaces sociaux, et il variait en fonction de ses motivations et des circonstances sociales, et ainsi en fonction du temps et du lieu. Les crimes commis dans le passé n'existent plus aujourd'hui et vice versa. De même, les crimes commis dans un lieu ne sont pas forcément ceux commis dans un autre lieu, et cela est dû à la différence qui existe entre les comportements des membres de la société en termes de niveau culturel, scientifique, matériel et parfois religieux.

La criminalité est un phénomène social, donc il est certain qu'il existe une similitude entre la cybercriminalité et la criminalité ordinaire dans ses trois éléments que sont la présence de l'auteur, de la victime et l'acte du crime. Considérant que le crime traditionnel est commis en présence de l'auteur et de la victime, et ce cas de crime se produit souvent dans un monde réel, les contrevenants agissent dans un contexte bien délimité; or la cybercriminalité est à l'opposé car elle se produit souvent sans que la personne qui commet le crime soit présente sur les lieux de l'événement ; et la victime peut ne pas être présente sur les lieux du crime et la méthode utilisée est la technologie moderne, les moyens de communication et les réseaux électroniques modernes et de ce fait on peut y croire aux déclarations de certains chercheurs qui confirment que l'internet présente «une opportunité unique pour un comportement déviant» (Rogers et Smoak.2006. pp245-268). Nous pouvons également comprendre que l'outil du crime ici est constitué de dispositifs numériques et d'informations avancées, contrairement à la criminalité traditionnelle, dans laquelle l'auteur ou le criminel recourt souvent à plusieurs outils qui varient selon les circonstances et le lieu du crime.

Avec l'éclosion d'une cybercivilisation qui ébranle les frontières de notre planète, on peut conclure que la cybercriminalité se caractérise par la globalité, car ces crimes sont commis dans un monde virtuel qui n'est pas limité par des frontières géographiques, ce qui rend extrêmement difficile la découverte de leurs auteurs.

Parmi les paradoxes qui apparaissent, les partisans du côté jurisprudentiel considèrent que la cybercriminalité se caractérise par la rapidité, la sophistication des moyens qui varie beaucoup; et parfois les cybercriminels font recours aux techniques et tirent parti des outils de sécurité commerciaux utilisés par les groupes de chercheurs en sécurité (Centre Canadien pour la cybersécurité.2022.p3), et l'absence de violence physique contre les personnes par rapport aux délits traditionnels lors de leur mise en œuvre.

En d'autres termes, la cybercriminalité est un phénomène mondial qui n'a pas de nationalité, de race ou de couleur spécifique, et ses risques dépassent de loin ceux des principales organisations criminelles connues dans le monde, et c'est ce qu'a déclaré le chef d'Interpol au sujet de l'ampleur et des dégâts économiques causés, les plus grands pays développés n'étaient pas exclus, et ce nonobstant leurs progrès remarquables en matière de technologies de l'information et de la communication, leur supériorité scientifique et leur solide arsenal législatif.

3/ **Impact et méfaits de la cybercriminalité par rapport à la criminalité traditionnelle :**

La diffusion croissante des technologies de l'information et de la communication, qui se sont développées sous la forme d'une suite géométrique, a permis l'émergence de nouveaux termes –appellations- auxquels nous ne sommes pas habitués, comme les technologies à ciel ouvert, qui ont détruit toutes les frontières géographiques à travers tous les continents, et cela a contribué, d'une manière ou d'une autre, à l'émergence de nouveaux comportements comme un réservoir intarissable d'opportunités frauduleuses (Benoît. 2013. pp.39-56).

4/Types de cybercriminalité :

Il est extrêmement difficile de parvenir à une définition précise des types de cybercriminalité, et la possibilité d'une stabilité pour certains types est devenue discutable, et le désaccord entre les chercheurs concernant la classification des délits électroniques est le résultat de l'émergence de nouveaux délits, car la cybercriminalité est quasiment indéterminée que nous ne pouvons la limiter à tous ses types et formes, et ils sont évolutifs et renouvelables, et chaque fois qu'une nouvelle façon d'utilisation des ordinateurs et Internet apparaît, un nouveau crime apparaît avec elle. Il est certain que tous les cybercrimes, quels que soient leur type et leur forme, ciblent bien entendu des individus, des groupes,

des institutions et des pays. A travers cette recherche, nous tentons d'illustrer tous types de cybercriminalité les plus courants et les plus répandus, qui se résume comme suit :

4-1) Crimes visant des individus : Il s'agit de délits par lesquels un préjudice est causé à un individu spécifique qui touche à son intégrité physique et psychologique ou à un groupe d'individus afin d'obtenir des informations importantes liées à leurs comptes, qu'ils soient bancaires ou sur Internet.

4-2) Crimes portant préjudice aux institutions : Ils sont sous le nom « crimes technologiques » qui visent un ordinateur ou un réseau informatique et il s'agit alors de crimes technologiques à proprement parler, ou même des biens personnels, sous le nom des crimes contre les biens. Ou encore, il est possible de voler les informations des employés d'institutions et d'entreprises, de les inciter et de les faire chanter afin de détruire les systèmes internes des institutions, d'installer des dispositifs d'espionnage sur les comptes et les systèmes et de chercher à les pénétrer et à les contrôler pour obtenir des gains matériels et politiques.

4-3) Crimes contre les gouvernements: Ce type de cybercriminalité consiste à pénétrer et à contrôler les sites Web d'entités officielles des pays, puis à les utiliser au profit d'entités dangereuses à travers lesquelles on cherche à déstabiliser la sécurité du pays, à contrôler l'esprit des jeunes et à les inciter à commettre des actes illégaux ; Il faut noter que plusieurs gouvernements se sont préoccupés de la réalité du cyberespace en émergence, car ils la considèrent comme une menace pour leur souveraineté (Enderlin. 2010-2011. p11).

5/ Causes et motivations de la cybercriminalité :

Il est certain que les auteurs de crimes électroniques ne sont pas nécessairement les mêmes que ceux qui commettent des crimes traditionnels, et cette différence peut être due à la différence de circonstances, d'outils, de moyens, de méthodes, d'actions ; et dans une autre mesure, peut être due à leur éducation, à leur niveau d'éducation, et certaines circonstances extérieures, et de ce fait nous essayons de mettre la lumière les plus importantes, qui sont comme suit :

5-1)Crimes d'argent : la principale raison qui motive la commission de ce crime électronique est la recherche de profits et de gains matériels, en faisant recours au piratage de comptes bancaires, ou des comptes liés aux institutions publiques et à d'autres institutions privées. Par exemple, l'année 1988 a été témoin d'une tentative de vol de fonds par des moyens électroniques, pour voler 80 millions de dollars américains de la banque « First National Bank of Chicago » مجمع البحوث والدراسات. 2019. ص9) (.

5-2) Piratage des informations : Le motif dans ce cas réside dans l'utilisation de logiciels et de technologies modernes pour saisir, modifier, et supprimer partiellement ou définitivement les informations stockées dans l'ordinateur par l'ordinateur. Et selon l'étude réalisée par Business Software Alliance (BSA) sur les taux de piratage de logiciels dans le monde en 2003, cette infraction atteint un taux de 37% dans l'Union Européenne. Son coût pour les éditeurs nationaux et internationaux a également été chiffré puisque la valeur des logiciels piratés dépasse 9,7 milliards de dollars. L'étude a montré aussi que 45% des logiciels utilisés par les entreprises étaient piratés (BSA. http://www.bsa.org/France/). De cette lecture, on conclut que le motif peut avoir le titre compétitif ou provoqué par le chantage ou l'obtention d'avantages et des gains.

5-3) Recherche de l'appréciation, de la supériorité et la distinction de soi : On retrouve sous ce nom un groupe de jeunes, par souci de challenge, et pour démontrer leur supériorité sur les moyens technologiques et ceci peut s'expliquer

par la satisfaction de leurs penchants égoïstes (Enderlin. 2010-2011.p28), et ils sont à l'origine passionnés par l'outil informatique et tentent de trouver un moyen de le détruire et même de le surpasser.

5-4) Chômage et conditions économiques : Certains décrivent que la cybercriminalité, comme la criminalité traditionnelle, est liée au chômage et aux conditions économiques; et dans les deux cas, les motifs sont toujours le même, voire le profit.

5-5) L'absence de législation encadrant le phénomène de la cybercriminalité : Selon certains avis, nonobstant une pléthore de définitions adoptées par certains pays dites européens, mais il s'avère qu'il ait des lacunes et aucun texte législatif ou réglementaire ne définit la cybercriminalité (Chawki. Essai sur la notion de cybercriminalité. http://www.iehei.org) ; on constate qu'il ya une disconvergence entre les lois et les textes adoptés de par les nations, tout les états se sont convenues que la cybercriminalité est synonyme de tout comportement illégal, or le paradoxe un comportement peut être considéré illégal dans un Etat et légal dans l'autre.

6/ les répercussions de la cybercriminalité :

6-1) Violations des droits humains : Ces dernières années, nous avons été témoins d'un type de cybercriminalité qui porte atteinte au caractère sacré et à la dignité de l'être humain.

On entend du jour en jour, par de nouveaux types de crimes commis via internet, toute société n'est à l'abri, et les parents sont de plus en plus inquiets, surtout qu'on entend des enlèvements et à la traite des êtres humains, le kidnapping, et au fil des jours et des grands moyens technologiques les réseaux sociaux sont devenus un basin et un lieu idéal pour le trafic et la pornographie, notamment celle liée au mineures; une enquête réalisée aux Etats-Unis indique que les réseaux internet renfermaient alors 450 000 images ou fiche de nature pornographique, et que ceux-ci avaient été consultés par 6 millions de reprises (Socchard.2021. P54).

Les deux dernières décennies ont également permis l'émergence de ce que l'on appelle le « cyberterrorisme international», où des groupes terroristes ont utilisé les médias sociaux pour recruter et attirer des éléments, les attirer via Internet et les recruter depuis leur domicile à travers le monde, formation militaire des membres recrutés et fabrication d'explosifs, conflits entre religions, races et couleurs humaines à travers le monde et à la promotion de discours de haine entre individus, entre groupes et même entre pays également, dans le but de semer le chaos et la confusion dans les sociétés, promouvoir des discours de haine contre l'islam, ou ce que l'on appelle « l'islamophobie ».

Il est évident, comme lecture sociologique, les comportements des cybercriminels sont alimentés par : facteur économique (gain et tirer profit) ; égocentrique (pour se faire du plaisir, la recherche de la reconnaissance sociale) ; idéologique (la revanche sur la société) ; psychotiques caractérisés par la perte du sens de la réalité (Bologna.1986) ; extrémisme (groupe et attentat terroriste).

6-2) les méfaits de la cybercriminalité sur l'environnement économique

Notre lecture approfondie sur ce thème nous a permis de constaté que certains analystes estiment que les dangers et les effets résultant de la criminalité électronique à tous les niveaux dépassent de loin les effets résultant de la criminalité traditionnelle. Selon certains rapports internationaux, l'économie mondiale subissait des pertes s'élevant à 2,9 millions de dollars chaque minute en raison de la cybercriminalité. Il est palpable que la cybercriminalité peut provoquer un effondrement économique mondial en 2019, la valeur des pertes résultant de ces crimes a atteint environ 945 milliards de dollars, soit l'équivalent de 1% de la production mondiale totale, soit une augmentation de 423 milliards de dollars par rapport à 2018, et ce selon les données de l'institution de cyber-sécurité « McAfee », qui est considéré

comme l'une des institutions de cyber-sécurité les plus importantes au monde (الجرائم الالكترونية تدق ناقوس الخطر. https://draya-eg.org/2022https://draya-eg.org/2022)

Selon certains rapports, le **coût mondial de la cybercriminalité** est de l'ordre de 1 000 milliards USD par an, soit 1% du PIB mondial (Atlas Magazine, cybercriminalité: coût économique et réactions des pouvoirs publics, décembre 2022. https://www.atlas-mag.net/category/tags/focus/cybercriminalite-cout-economique-et-reactions-des-pouvoirs-publics#). Pour illustrer les méfaits et l'impact de la cybercriminalité sur l'économie mondiale, on croit que c'est l'heure de tirer la sonnette d'alarme, et selon le même rapport, il ya environ 1000 milliard USD de perte économique en 2021, soit une hausse de 15% par an de dommages économiques, un temps d'arrêt moyen par entreprise de 24 jours, et un montant de primes assurance de 10,33 milliards USD comme coût bilatéral (Rapport de Coveware Allianz. Deuxième trimestre2022).

Il faut aussi noter La société *McAfee* (spécialisée dans la sécurité informatique) et le *Center for Strategic and International Studies* ont diffusé en juin 2014 un rapport qui estime le coût du préjudice financier causé par la cybercriminalité à 445 milliards de dollars par an dans le monde ; et il est estimé en l'année 2023 - selon quelques statistiques- qu'on aurait une moyenne de 667 milliards de dollars par mois, soit 154 milliards de dollars par semaine, 21,9 milliards de dollars par jour, environ 913. 1 million de dollars par heure (خالد وليد. الجرائم الالكترونية كظاهرة عالمية. https://www.aljazeera.net/opinions/2023) ,et selon deux études menées par le FBI et IBM en 2006, la cybercriminalité coûte 67 milliards de dollars par an rien qu'aux États-Unis, soit environ 2 millions de dollars par minute. (Drothier.2006)

Certes, il est quasiment impossible de connaitre les chiffres réels des méfaits de la cybercriminalité, mais ce qu'il faut retenir que personne ne peut à l'abri de cyberattaque et ses impacts infectent non seulement la vie économique, mais aussi la vie sociale et psychologique des personnes ou des institutions.

***7/* Les répercussions de la cybercriminalité sur la sécurité internationale :**

Il est évident avec l'augmentation du nombre d'utilisateurs d'Internet et le développement des technologies de la communication et de l'information, le volume de la criminalité électronique a aussi augmenté, et ce sous plusieurs formes ; y compris le piratage électronique, qui a traversé toutes frontières et a atteint un plus haut niveau, dont les tâches sont accomplies par des spécialistes et des ingénieurs de haut niveau, et ce, non seulement pour protéger leur sécurité nationale, mais aussi à des fins offensives et d'espionnage entre pays, notamment entre les pays développés, qui ont contribué, d'une manière ou d'une autre, aux attaques contre les plus grandes institutions gouvernementales et aux conflits entre pays.

Le cas le plus célèbre survenu ces dernières années, qui a provoqué un grand tollé et des conflits même entre pays amis et alliés, est peut-être le programme d'espionnage israélien «Pegasus». Des rapports internationaux ont récemment circulé sur l'utilisation du programme d'espionnage «Pegasus», pour pirater les téléphones portables- intelligents- des chefs d'État et de gouvernement, des ministres, des responsables, des militants, des opposants et des plus grands journalistes du monde.

8**) Aspects de la cybercriminalité au niveau mondial :**

L'avis commun de plusieurs auteurs qui ont travaillé sur ce sujet, estime qu'il est quasiment impossible de quantifier les pertes subies par le monde, tout comme il est extrêmement complexe de limiter l'identification des victimes, et les équipements de cybercriminalité. Et il demeure qu'aucune enquête ne peut être fiable car de nombreuses

entreprises ne communiquent pas sur les attaques subies, par peur de nuire à leur réputation (Monnet et Véry. 2013. P213)

Les estimations indiquent que l'économie mondiale basée sur Internet génère environ trois mille milliards de dollars par an, et ce chiffre est susceptible d'augmenter fortement dans les décennies à venir, et la criminalité électronique affecte un pourcentage compris entre 11 et 29 % de la taille de l'économie mondiale basée sur Internet (http://www.alhadath.ps/article/34 870.مليار دورلارخسائر الاقتصاد العالمي من الجريمة الالكترونية), et son impact s'accroît à la fois de manière horizontale et verticale.

Pour confirmer cette supposition, et selon le Forum Economique Mondial, le marché mondial clandestin du médicament est estimé à 145 milliards d'euros, un médicament sur deux vendus sur l'Internet est faux (Bureau de l'information et de la communication, DNRED. Lutte contre la vente illicite de médicaments sur internet. http://www.douane.gouv.fr/articles/a12030-lutte-contre-la-vente-illicite-de-medicaments-sur-internet) ; 23 % des entreprises ont été victimes de cybercrimes seule aux USA (Ducary. 2013); et entre autres, selon le 8e rapport annuel publié fin 2012 , l'Observatoire national de la délinquance et des réponses pénales (ONDRP) a recensé 33299 infractions qualifiées de «délinquance astucieuse » sur l'Internet dont 80 % étaient des escroqueries ou des abus de confiance, les 20 % restant correspondaient à des falsifications ou usages de cartes de crédit (Symantec. Etude Norton 2012 : coût de la cybercriminalité en France. http://www.symantec.com/fr/fr/about/news/release/article.jsp?prid=20120917_01).

Il est évident, que le cybercrime parcouru et franchi aussi d'autres pistes, comme celles liées au trafic de drogue, de prostitution, de blanchiment d'argent ou encore l'espionnage industriel, auquel s'ajoute aussi le cyberterrorisme qu'on l'en voit lors des guerres en Irak, Syrie et autres pays par des cellules spécialisées pour le recrutement via divers diversement ; et on entends parler à travers la presse mondiale de certaines attaques qui ciblent des infrastructures stratégiques d'un État telles que les infrastructures énergétiques, les réservoirs d'eau, les télécommunications et les banques, entraînant de graves répercussions pour la société. (Ghernaouti et Solange. 2002).

Auquel on ajoute la cyberguerre, qui enfin concerne les forces armées et fait référence à l'informatique dans l'organisation militaire, et leur but est de perturber autant que possible le fonctionnement des opérations militaires ou tout ce qui peut contribuer à diminuer la capacité à se défendre.

9/Conclusion et recommandations :

La cybercriminalité a pris, au fil du temps, de nouveaux types, et chaque fois que tous les pays du monde se précipitent pour adopter des lois, promulguer des lois et établir des programmes électroniques pour y faire face, de plus en plus ces crimes sont devenus plus graves, et plus ils deviennent dangereux en détruisant l'entité des personnes, des institutions et des pays en raison des dommages psychologiques, moraux et économiques qu'ils subissent, et on craint que cela se transforme bientôt en une porte d'entrée vers des conflits, des tensions, et les guerres entre pays.

Nous concluons également qu'il existe des lacunes dans les lois traditionnelles en vigueur dans certains pays, et que leur révision et leur modification ne sont pas la hauteur du rythme des développements et des innovations rapides survenues, notamment dans le domaine des médias, de la communication, et l'informatique.

Dans l'objectif de réduire et de limiter de leur propagation et de leur expansion dans le temps et dans l'espace, nous recommandons ces suggestions, peut-être qu'elles pourraient être utiles et efficaces, que nous résumons comme suit :

- La nécessité d'une coordination et d'une coopération internationale et régionale, judiciaire et procédurale, dans le domaine de la lutte contre la cybercriminalité et des technologies de l'information.
-Accélérer la coopération internationale pour lutter contre ce crime du point de vue procédural, dans le but de concilier les législations liées à ces crimes, comme la coopération internationale en matière d'échange d'informations et d'extradition de criminels ;
-l'introduction de certaines dispositions de la loi pour combler les lacunes et suivre le rythme du développement technologique et de ses outils de façon permanente ;
- Introduite une surveillance au sein des cybers-cafés et établir des contrôles qui limitent leur travail anarchique ;
- Introduire une surveillance au sein des cybers-cafés et établir des contrôles qui limitent leur travail anarchique ;
- Développer les capacités des ressources humains travaillant dans les domaines de la lutte contre la délinquance informatique afin de suivre le rythme des évolutions technologiques successives ;
- La nécessité de créer une nouvelle culture sociale qui dénonce les crimes sur Internet, tout en activant la méthode de sensibilisation parmi les utilisateurs du réseau mondial de communications ;
- Insérer des cours sur la criminalité électronique et les moyens d'y faire face dans les programmes d'études scolaires et universitaires, créer un sujet sur «l'éthique de l'utilisation d'Internet» et l'inclure dans les programmes éducatifs pour sensibiliser et donner aux enfants et aux jeunes des attitudes positives à l'égard de l'utilisation d'Internet ;
- Intensification des campagnes médiatiques pour sensibiliser les individus du danger de la cybercriminalité et à la manière de protéger leurs appareils numériques ;
- Encourager les universités et les centres de recherche à organiser des séminaires et conférences traitant le développement de la cybercriminalité et des moyens de la combattre et d'en limiter les effets;
- Activer le rôle des organisations de la société civile pour sensibiliser et alerter sur les dangers d'Internet et de la criminalité numérique via Internet.

Bibliographie :

I)Listes des ouvrages et documents en français

1- B. Monnet et P. Véry. (2010). *Les nouveaux pirates de l'entreprise*. CNRS. Paris.
2- Clément , Enderlin. (2010-2011).les moyens juridiques et institutionnels nationaux et européens de lutte contre la cybercriminalité dans le cyberespace. Mémoire de recherche, Institut d'études politiques de Strasbourg.
3- Centre Canadien pour la cybersécurité. (2022). Introduction à l'environnement de cybermenace 2023 /2024- journal du centre de la sécurité des communications, Ottawa, Canada.
4- David Ducary, Hétu. (2013). Piratage information, Cyberciminalité entre inconduite et crime organisé. Presse internationale polytechnique. Canada.
5- D-B, Parker. (1985). combattre la criminalité informatique. Paris, ros.
6- G-J, Bologna. (1986). An Organizational Perspective on Enhancing Computer Security. Communication au Congrès Securicom.

7- Ghernaouti-Hélie, Solange. (2002). Internet et sécurité. coll. Que sais-je?

8- H. ATERMAN et A. BLOCH. (3 sep. 1988). La Fraude Informatique . Paris, Gaz. Palais.

9- LIANG, Jiansheng. (1999). criminalité informatique. Diplôme professionnel supérieur en sciences de l'information. école supérieure des sciences de l'information et des bibliothèques- ENSSIB-Villeurbane.

10- P –M. REVERDY. (2005). La Matière pénale à l'épreuve des nouvelles technologies.Thèse de Doctorat, Université Toulouse I.

11-Schell, B.H et C.Martin. (2004). Cybercrime : A reference Handbook, Sanra Barabara, Etats- Unis: ABC-CLIO

12- Rogers, M t Smoak, N. (2006). & Liu, J. Self-reported deviant computer behavior. Deviant Behavior. 27(3)

13- Sébastien, Socchard. (2019). les intrus sont parmi nous. Abstract UNIX.

14- S, El ZEIN. (2006, 24 janvier). L'Indispensable Amélioration des Procédures Internationales pour Lutter Contre la Criminalité Liée à la Nouvelle Technologie in M.-C. Yves Drothier. « *Le cybercrime à l'origine d'une perte de 67 milliards de dollars aux États-Unis* ». sur Le Journal du Net

15-Atlas Magazine, cybercriminalité: coût économique et réactions des pouvoirs publics, décembre 2022, disponible sur site : https://www.atlasmag.net/category/tags/focus/cybercriminalite-cout-economique-et-reactions-des-pouvoirs-publics#

16- Bureau de l'information et de la communication, Direction nationale du renseignement et des enquêtes douanières. (2014) . Lutte contre la vente illicite de médicaments sur internet. http://www.douane.gouv.fr/articles/a12030-lutte-contre-la-vente-illicite-de-medicaments-sur-internet.

17-David, Décary-Hétu. (2020,08 juillet). la cybercriminalité. https://www.crimrxiv.com/pub/zk9k26ba/release/1

18- BSA. (02-janvier 2024à). www.bsa.org/France.

19-Symantec. (2012). coût de la cybercriminalité en France. Etude Norton. http://www.symantec.com/fr/fr/about/news/release/article.jsp?prid=20120917_01.

20- Gagnon, Benoit. (2002, 12 mai). Le cyberterrorisme à nos portes. La Presse.A15. http://www.dandurand.uqam.ca/download/journaux/gagnonb/20020512.htm

21- Mohamed Chawki. Essai sur la notion de cybercriminalité. http://www.iehei.org

II) Liste des ouvrages et documents en arabe

22-عادل يوسف عبد النبي الشكري.(2002). نقلا عن: كتاب- الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها-، إعداد مجمع البحوث والدراسات. نزوى. سلطة عمان.

23- الجرائم الالكترونية تدق ناقوس الخطر. /https://draya-eg.org/2022

24- خالد وليد محمود، الجرائم الالكترونية كظاهرة عالمية.https://www.aljazeera.net/opinions/2023

25- مليار دولار خسائر الاقتصاد العالمي من الجريمة المنظمة.http://www.alhadath.ps/article/34 870