CYBER-ARMES, QUELLE LÉGISLATION POUR LES ARMES IMMATÉRIELLES ?

Stéphanie AUBERT

Chargée d'enseignement à l'Université Panthéon – Assas,
Chef d'entreprise AS Conseil, Intelligence économique et juridique
et

Thierry AUTRET

RSSI Groupement des Cartes Bancaires CB

« Les armes sont des instruments qui servent à porter des coups et à les parer, comme sont les épées et les mousquets que l'on appelle armes offensives et les boucliers et les cuirasses que l'on appelle défensives »[1].

Depuis que le monde est monde, les esprits malins se sont évertués à détourner les technologies inventées par l'homme à leur profit. Le début du XX[e] siècle a vu apparaître l'utilisation de l'automobile par la « bande à Bonnot » pour échapper aux policiers à bicyclette ou celle de la dynamite volée sur les chantiers pour ouvrir les coffres-forts des banques. N'échappant pas à ce principe, l'informatique à son tour est devenue tour à tour un média, un moyen ou une cible utilisé par les fraudeurs. La généralisation de l'informatique dans tous les domaines de la vie courante associée à la connaissance des techniques, de plus en plus répandue dans les écoles, entraîne une multiplication des sources de menace.

Basé sur les principes de la machine de Turing, un logiciel est un ensemble d'instructions interprétées par un processeur afin de réaliser des traitements sur des données. Les logiciels, qu'ils soient au niveau matériel comme le BIOS, au niveau système comme Linux ou Windows, ou au niveau d'une l'application comme un gestionnaire de base de données, sont l'intelligence de nos ordinateurs, de nos téléphones, de nos voitures. Mais les logiciels sont-ils vraiment intelligents ? Ils traduisent seulement l'intelligence de leurs concepteurs en leur apportant la rapidité de calcul que seule une machine est capable d'offrir.

Mais si le développeur est malhonnête, alors le logiciel qu'il développe traduira sa malice, sa propension à faire le mal. Son logiciel devient alors un maliciel, un logiciel destiné à perturber, altérer ou détruire tout ou partie du système d'information qui est devenu sa cible. Comme le chasseur qui vise sa proie avec une arme, le malfaiteur vise le système d'information qu'il cible avec une arme informatique. Mais paradoxalement, contrairement à un arc et ses flèches ou à une carabine et ses cartouches qui peuvent également être utilisés à des fins de loisir

[1] Dictionnaire de droit civil et de pratique, Paris, 1687.

sportif, le maliciel n'a pas d'autre destination alternative que de pénétrer, espionner des systèmes d'information, et exfiltrer des données.

L'alinéa premier de l'article 132-75 dispose qu' « est une arme, tout objet conçu pour tuer et blesser ». Ainsi de prime abord, l'arme détient une matérialité tangible servant un but ultime : la violence. Le Code pénal va plus loin en distinguant selon les circonstances : certaines armes le sont par nature selon l'alinéa 2 tandis que d'autres le sont par destination en fonction de l'usage que la personne détentrice entend en faire selon l'alinéa 3. Mais pour autant, les finalités restent les mêmes : blesser ou tuer.

Une arme à feu est sans conteste une arme par nature alors qu'un bâton a été défini selon la jurisprudence comme étant une arme par destination. Ces évidences heurtent une réalité plus obscure, celle de la cyberguerre et de la cyberdélinquance.

Justement, elle désigne la délinquance liée aux systèmes et réseaux numériques. Plus précisément, ce sont toutes les formes de délinquance qui concerne les situations dans lesquelles les systèmes informatiques constituent l'objet même du délit ainsi que la délinquance qui concerne les situations dans lesquelles les systèmes ou les réseaux informatiques constituent le moyen de commettre l'infraction. Le droit français a appréhendé très tôt le phénomène avec la loi GODFRAIN de 1988 sur les atteintes aux systèmes de traitement informatisé de données (STAD) mais la loi du 9 mars 2004 marque un pas supplémentaire en s'attardant sur la cryptologie, c'est la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Notre arsenal est complété, suite aux attentats du 11 septembre 2001, avec la loi sur la sécurité quotidienne (LSQ) de 2001 qui a permis la conservation des données pendant un an. La loi de mars 2004 a renforcé les moyens d'investigation dont les perquisitions informatiques et les interceptions téléphoniques transposables à Internet. La loi LOPPSI II a introduit l'infraction relative au délit d'usurpation d'identité.

La conception de la violence dans le cadre de la cyber-délinquance est difficilement acceptable et la notion d'arme immatérielle souffre donc d'un manque de reconnaissance. Pourtant, le législateur et le monde des praticiens du droit n'hésitent pas à parler d'agression ou encore de dommage. Le lien de causalité est donc très distendu. Il convient pour ce faire de repenser l'article 132-75 du Code pénal dans son intégralité pour y inclure cette nouvelle acception de l'arme.

Le Livre blanc Défense et Sécurité Nationale – 2013 rappelle que la situation est préoccupante car ce sont des millions d'euros et des milliers de jours homme qui sont dépensés par les entreprises qui subissent des attaques informatiques. Mais aujourd'hui, le politiquement correct interdit de nommer l'adversaire ou l'ennemi en qualifiant des malfaiteurs multirécidivistes poursuivis pour des atteintes aux biens de « frères égarés commettant des incivilités ».

Les atteintes aux systèmes d'information sont encore trop souvent considérées par les entreprises comme des défaillances de leurs protections, maintenant qualifiées de mauvaise « hygiène informatique » (réf. Patrick Pailloux ANSSI). Pour ce type de méfaits, les entreprises et les particuliers ne prennent pas suffisamment conscience qu'ils sont victimes. Ils sont rarement recensées au titre de crimes ou délits dans l'état 4001 des faits constatés, alimenté par les forces de l'ordre police ou gendarmerie et géré par la direction centrale de la police judiciaire (DCPJ). Et pourtant en 2011, l'Observatoire national de la délinquance et des réponses pénales (ONDRP) fait déjà état de 33.000 cyber-infractions déclarées dans son rapport annuel sur l'état de la criminalité en France.

Il est donc primordial de repenser la violence et l'arme pour appréhender au mieux cette délinquance et pour y apporter une réponse juridique appropriée. Comment peut-on traduire juridiquement ces armes inédites ?

I. Le maliciel comme arme de nouvelle génération

Traiter le maliciel comme une arme selon les termes de l'article 132-75 n'est juridiquement pas concevable de prime abord tant nous sommes éloignés de sa conception classique. Or, « la loi pénale est d'interprétation stricte » selon l'article 111-4 du Code pénal. Il est donc impossible d'étendre la caractérisation au logiciel malveillant à moins de réécrire cet article ou d'en changer l'esprit.

A. La caractérisation de l'arme par destination refusée

La catégorie des armes par nature comprend tous les objets que l'industrie humaine n'a pas destinés à d'autres fins que celle d'être des armes. Il en est différemment des armes par destination qui ne sont des armes que par l'usage que l'on en fait. En effet, elles sont détournées de leur usage quotidien non agressif en vue de tuer ou blesser. Dans cette seconde catégorie, il est induit *de facto*, que la dangerosité n'est pas incluse ; elle se gagne.

Or, un maliciel de par son existence, est malveillant. Il est nuisible dès sa création et n'est donc pas détourné de son usage. En cela, il se rapprocherait plus d'une arme par nature, dangereuse *ab initio*.

Pourtant, aucune des deux qualifications n'est opérante dans la mesure où les finalités octroyées à l'arme ne sont transposables au maliciel. En effet, l'article 132-75 spécifie bien que l'arme doit « tuer ou blesser ». En effet, il n'y a que métaphoriquement que le maliciel peut avoir d'impact directement mortel. Mais selon un raisonnement téléologique, privilégiant l'esprit de la loi, on ne peut que douter que le législateur avait en tête des objectifs figurés à l'arme.

Pourtant, très récemment, le nouveau décret n° 2013-700 du 30 juillet 2013 portant application de la loi n° 2012-304 du 6 mars 2012 relative à l'établissement d'un contrôle des armes moderne, simplifié et préventif, introduit une nouvelle définition de l'arme : « tout objet ou dispositif conçu ou destiné par nature à tuer, blesser, frapper, neutraliser ou à provoquer une incapacité ». Le décret ne précise pas si la destination de l'arme s'applique à des personnes ou à des biens. Dans notre cas, « neutraliser ou provoquer une incapacité », si tant est que cette définition peut s'appliquer à des biens, correspondrait aux conséquences d'un déni de service résultant d'une attaque DDOS ou d'un blocage des activités métier par infection du système d'information par un virus.

Il n'est donc pas recevable « en l'état » de considérer le maliciel comme une arme à moins de réécrire l'article 132-75. C'est d'autant plus vrai qu'il se situe dans la section III du livre 1er intitulée « De la définition de certaines circonstances entraînant l'aggravation, la diminution ou l'exemption des peines ». Il est donc clair que l'usage de l'arme est une circonstance aggravante, une variable d'ajustement de l'infraction principale. L'intérêt est double dans la mesure où, soit l'usage de l'arme entraîne une augmentation de la peine, soit elle opère un changement de qualification.

Or, l'usage du maliciel constitue l'objet même de l'infraction et non pas un moyen de parvenir au résultat de l'infraction, se rangeant du côté des infractions

formelles et non matérielles. La matérialité est donc bien la détention et l'utilisation de ce logiciel malveillant, lui niant par là-même la qualité de circonstance aggravante.

Pour autant, cela laisse quand même un champ d'application pour une réécriture lorsque le maliciel n'est qu'un moyen de parvenir à une matérialité précise.

B. La violence repensée

Parler de cybercriminalité est une bonne chose car c'est la reconnaissance d'un phénomène, minimisé jusqu'à présent en raison de la virtualité des dommages. Mais sémantiquement, c'est une méprise de la situation. En effet, l'article 111-1 du Code pénal fait état d'une classification tripartite des infractions. Dans cette optique, il est réducteur de ne parler que de l'infraction la plus grave et de laisser de côté le délit et la contravention. Il conviendrait d'utiliser le terme générique de cyber-délinquance.

La délinquance induit un trouble à l'ordre public causé par un acte de violence dirigé soit contre des personnes soit contre des biens. Sur ce point, nous devons élargir notre champ de vision en admettant des violences qui ne sont ni physiques ni morales. En réalité, admettre le maliciel comme une cyber-arme induit de définir des violences immatérielles. On se situe alors, dans un mouvement plus large consistant à transposer le droit pénal général au domaine immatériel.

La première illustration est la reconnaissance jurisprudentielle du vol d'information. L'arrêt de la Chambre correctionnelle du Tribunal de Grande Instance de Clermont Ferrand en date du 26 septembre 2011 est particulièrement éclairant. Alors que la Cour de Cassation a toujours refusé d'appliquer la notion de vol à l'information sans support matériel, le TGI en juge autrement lorsqu'il décide de condamner une employée pour abus de confiance et vol de données informatiques. Selon lui, les faits étaient établis. Si l'accusation d'abus de confiance a déjà été retenue par le passé, celle de vol de données immatérielles est nouvelle. Aux termes donc de l'article 311-1 du Code pénal, le vol consiste en « la soustraction frauduleuse de la chose d'autrui ». Le TGI considère que « le transfert d'informations aux fins d'actualisation des fichiers sont constitutifs de soustraction frauduleuse ». Il convient de rapprocher cette évolution de celle qui tend à reconnaître un secret des affaires, notamment par un projet de loi.

La seconde est l'admission de la notion de bien immatériel pour consacrer définitivement l'infraction de cyber-terrorisme. Sur ce point, il convient de réfléchir sur la notion de délinquance-moyen (dans l'affaire MERAH, le jeune homme s'est servi d'Internet pour commettre ses méfaits) et de délinquance-objet (attaques sur des points d'importance vitale, déni de service). Dans la première hypothèse, il s'agit d'un crime de droit commun qui a utilisé le cyberespace comme moyen de propager l'action terroriste soit par la propagande soit par le financement. Dans la seconde hypothèse, ce sont des actions terroristes directement menées dans ce nouveau territoire. STUXNET a, de ce fait, mis fin à l'angélisme qui régnait tendant à considérer que seuls des hackers fous pouvaient mener ce genre d'opérations. Il est alors patent que le cyber-terrorisme ne vise que cette seconde tendance et consacrerait une vision élargie de ce crime de droit dérogatoire.

La violence immatérielle peut alors être définie comme celle causant des nuisances et des dommages aux systèmes d'information de façon simpliste. Les

attaques peuvent avoir des conséquences sur les éléments essentiels de cette société de l'immatériel : la confidentialité, l'intégrité et la disponibilité des données. Il est aisé de faire un parallèle avec ce que nous connaissons en matière de personne physique. Elles peuvent en perturber le fonctionnement avec le déni de service ou d'accès. Enfin, elles peuvent propager des contenus illégaux. Ses impacts sont considérables et multiples, comme des pertes financières pouvant entraîner des faillites d'entreprises et des pertes d'emplois, des vols d'identité pouvant briser la vie de la victime, voire dans des cas extrêmes entraîner indirectement la mort de personnes physiques[2] (cas STUXNET). Plus récemment, un chercheur à démontré pouvoir prendre la main sur un pacemaker et le perturber jusqu'à envoyer une décharge pouvant causer la mort[3]. Dans ce cas extrême ce type de maliciel deviendrait à proprement parler une arme au sens juridique. Pourtant, cette éventualité n'est pas permise actuellement à moins de faire évoluer les nomenclatures déjà existantes.

C. De la question du double usage

Les méthodes et outils d'attaques des systèmes d'information sont polymorphes. Ils combinent l'exploitation de failles des systèmes analysées par des outils logiciels automatiques ou scanner de ports (Nessus, Snort...), des maliciels (keyloggeur, zombies/botnet, virus, vers, etc.), auxquels s'ajoute le savoir faire des attaquants (APT ou Advanced persistant threat) [6].

Mais le problème est plus complexe. En effet, les sociétés qui vendent des services d'audit de systèmes d'information, communément appelés tests de vulnérabilité et tests de pénétration, utilisent en partie les mêmes outils ou savoir-faire (en dehors des maliciels). Ils le font dans un cadre contractuel avec leurs clients et selon une éthique stricte[4] et ne doivent pas être poursuivi pour cela.

Juridiquement, ils sont définis à l'article 2 du règlement communautaire n° 428/2009 du 5 mai 2009 : « les produits, y compris les logiciels et les technologies susceptibles d'avoir une utilisation tant civile que militaire ». On retrouve nos maliciels dans les catégories 3 « électronique » ou 5 « télécommunications et sécurité de l'information ».

Sur un autre angle très similaire, le séminaire gouvernemental sur le Numérique a évoqué dans la Feuille de route du Gouvernement sur le Numérique du 23 février 2013, dans sa Mesure n° 18, le constat que les technologies de surveillance et de contrôle de l'Internet peuvent « [...] permettre à des régimes autoritaires de limiter l'exercice des Droits de l'Homme et notamment de la liberté d'opinion et d'expression. », mais que dans le même temps « Ces outils sont également largement utilisés pour des activités commerciales de mesure d'audience ou d'analyse de trafic [...] ». Cette mesure conclue ainsi, « L'objectif du Gouvernement est d'inclure les technologies de surveillance et de contrôle de l'Internet dans la liste des biens à double usage dont l'exportation est soumise à autorisation. ».

---

[2] Quelques personnes auraient été tuées lors de la destruction de centrifugeuses d'enrichissement d'uranium visées par l'attaque STUXNET.

[3] SC Magazine : un chercheur australien, BARNABY JACK, a démontré comment pirater un pacemaker lors du Congrès de BREACKPOINT 2012.

[4] Ce type d'activité est parfois désigné sous l'appellation « *éthical-hacking* ».

Sur ce double usage possible des logiciels il convient de rappeler l'article 323-3-1 (issu de la loi du 21 juin 2004 pour la confiance dans l'économie numérique) du Code pénal sur la détention de programme informatique malveillant qui dispose que :

« Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

La matérialité de l'infraction est constituée dans cinq cas bien précis ce qui en fait une infraction de commission intentionnelle avec un dol spécial, celui de commettre des infractions nommées aux articles 323-1, 323-2 et 323-3 réprimant respectivement l'accès frauduleux, l'entrave au fonctionnement et la modification frauduleuse de données dans ou contre un STAD (voir chapitre 7.1.2.). Ce qui est étonnant est la répression d'une sorte de complicité qui n'exige pas de fait principal mais seulement la fourniture de moyens spécifiquement préparatoires d'une des infractions citées au sens de l'article 121-7 du Code pénal réprimant la complicité.

L'expression « sans motif légitime » est bien la clé du problème. C'est une cause d'irresponsabilité pénale spécifique mais son appréciation peut laisser libre cours à l'imagination du juge. L'arrêt du 27 octobre 2009 de la chambre criminelle de la Cour de cassation témoigne de cette difficulté[5] en décidant qu'un « prévenu ne pouvait arguer d'un motif légitime tiré de la volonté d'information dès lors, que du fait de son expertise, il savait qu'il diffusait des informations présentant un risque d'utilisation à des fins de piratage ». Or, les informations étaient visibles sur le site de la société, ainsi le risque d'utilisation frauduleuse est suffisant pour écarter ce motif légitime. L'argument tiré de sa compétence ne vient que corroborer le refus d'invoquer cette cause d'irresponsabilité. Il est donc patent que la Haute juridiction entend limiter le champ d'application de ce motif légitime.

Dans le cas des logiciels, le législateur a voulu par cette expression protéger les besoins de la recherche scientifique et les besoins de protection de la sécurité des réseaux et systèmes d'information. En revanche, le malfaiteur qui utilise un maliciel pour pénétrer un système d'information et voler des données le fait au seul motif illicite du vol.

Ainsi, les biens ou technologies à double usage peuvent être qualifiés d'armes immatérielles dans leur usage délictuel. Mais pour une caractérisation plus pertinente, il convient de ne plus appliquer le fait justificatif tiré du motif légitime. Ainsi, il y aurait un alignement sur l'article 132-75 et une application dans la droite ligne des autres faits justificatifs communément admis. Ce serait une assimilation normale et un pas vers la reconnaissance de l'arme immatérielle comme peut l'être l'arme par nature.

II. Une classification pour les armes immatérielles

Un article de Thomas Rid et Peter McBurney de 2012 s'attache à définir ce qu'est une cyber-arme [8]. Ils rappellent qu'il n'y a pas de définition claire des

[5] N° pourvoi : 09-82346.

armes aux États-Unis et proposent une définition proche mais plus ouverte que la définition française : « une arme est un outil utilisé ou conçu afin de menacer ou de causer des dommages physiques, fonctionnels ou psychologiques à des structures, des systèmes ou des êtres vivants ». Dans leur article les auteurs font la distinction entre les termes anglais « arm » et « weapon ». Ils donnent au premier une conception large de l'arme, du lance-pierre au missile, alors qu'ils interprètent le second dans sa conception purement militaire. Voyons si le droit positif français connaît cette *summa divisio*.

A. Classification actuelle des armes

Jusqu'à l'été 2013, la classification des armes était régie par l'article 2 du décret 95-589 du 6 mai 1995 relatif à l'application du décret[6] du 18 avril 1939 fixant le régime des matériels de guerre, armes et munition – NOR: DEFC9501482D.

Depuis le 30 juillet 2013, celui-ci est abrogé par le décret n° 2013-700 portant application de la loi n° 2012-304 du 6 mars 2012 relative à l'établissement d'un contrôle des armes moderne, simplifié et préventif.

Il intervient en support du code de la défense article L.2331-1 sur sa partie régissant les armes et sa loi modificatrice la plus récente, à savoir la loi n° 2012-304 du 6 mars 2012 relative à l'établissement d'un contrôle des armes moderne, simplifié et préventif. Cette loi permet de définir les dispositions relatives aux conditions d'acquisition et de détention des armes de telle ou telle catégorie. Ainsi, des critères comme l'âge, les mentions au casier judiciaire ou la fonction entrent en ligne de compte. Croisés avec le type de catégorie d'arme, ils définissent les conditions pour leur acquisition ou détention.

Cette nouvelle classification comporte quatre catégories (A à D) sur lesquelles le législateur se base pour réglementer leur acquisition, détention, transport ou utilisation. Par exemple, les « armes à feu et leurs munitions conçues pour ou destinées à la guerre terrestre, navale ou aérienne » sont dans la catégorie A alors que les « armes et munitions historique et de collection » sont dans la catégorie D.

Parmi ces quatre catégories, il est intéressant de s'attarder sur la catégorie A2, à savoir les « matériels destinés à porter ou à utiliser au combat les armes à feu ». Curieusement, cette catégorie inclut aussi bien « 7° Les engins nucléaires explosifs [...] » que les matériels de visée nocturne ou les outils de chiffrement.

Sont ainsi classifiés d'arme de catégorie A2 : [extrait]

12° Matériels de transmission et de télécommunication conçus pour les besoins militaires ou pour la mise en œuvre des forces et leurs logiciels spécialement conçus ; matériels de contre-mesures électroniques et leurs logiciels spécialement conçus ;

13° Moyens de cryptologie spécialement conçus ou modifiés pour porter, utiliser ou mettre en œuvre les armes, soutenir ou mettre en œuvre les forces armées ;

[6] Modifié par le Décret n° 2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie.

Nous pouvons en déduire deux enseignements. Le premier est la juste prise en compte de la dangerosité de ces méthodes au rang des matériels de guerre, mais il est mis à mal par l'accumulation brouillonne d'armes, second enseignement. De plus, la cohérence n'est pas claire et cela peut nuire à l'exigence de sécurité juridique et d'intelligibilité de la loi.

B. Classification des armes immatérielles

Le législateur a donc considéré les dispositifs de transmission et les logiciels de chiffrement comme des armes de catégorie A2 alors qu'ils ne servent pas directement à tuer ou à blesser. Les dispositifs évoqués aux alinéas 12° et 13° contribuent potentiellement à la facilitation ou la mise en œuvre d'armes. L'ancêtre de l'ANSSI, à l'époque où elle s'appelait la DCSSI, s'était pour sa part appuyée sur les textes relevant des dispositifs à double usage pour réglementer fortement l'usage de la cryptographie.

Dès lors, un parallèle évident peut se faire avec les armes immatérielles. Nous retiendrons pour notre part la suggestion de Thomas Rid et Peter McBurney qui déduisent que les cyber-armes sont une sous catégorie des armes, et en donnent la définition suivante par analogie : « un code informatique utilisé ou conçu afin de menacer ou de causer des dommages physiques, fonctionnels ou psychologiques à des structures, des systèmes ou des êtres vivants. ».

Pour sa part, la Directive du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information décrit à l'article 7 les moyens d'attaque des systèmes d'information dans les termes suivants : « Outils utilisés pour commettre les infractions : [...] prendre les mesures nécessaires pour ériger en infraction pénale la production, la vente, l'utilisation [...] d'un programme informatique, conçu pour commettre une infraction. »

Par rapport à la rédaction de l'article 323-3-1 du Code Pénal qui est très proche, vient s'ajouter un fait important qui est la production, en fait la conception même de l'outil utilisé pour commettre l'infraction.

Nous pouvons dès lors considérer comme armes immatérielles les outils légitimes permettant d'effectuer des tests de vulnérabilité ou de pénétration mais aussi les logiciels de type maliciels dont la seule finalité est illicite. Bien entendu pour ces derniers il n'est pas question d'autoriser leur usage mais au contraire de disposer d'un référentiel sur lequel concevoir des réglementations d'interdiction.

C. La lutte informatique défensive et offensive

La lutte informatique défensive (LID) aussi bien qu'offensive (LIO) ont été introduites par le livre blanc de la défense et de la sécurité nationale de 2008 en leur fixant une priorité d'ici 2025 comme « clé de la supériorité opérationnelle ». Il est fort à penser que la nouvelle version de 2013 les évoquera également.

Les positions américaines sont encore plus tranchées dans les déclarations de politique défensive et offensive du Président Barack Obama. Ces positions sont décrites dans les propos que tient Harold Koh, le conseiller juridique du Département d'État U.S. , en disant que « l'État peut répondre à une cyberattaque en utilisant son droit de légitime défense tel que défini par l'article 51 de la charte des Nations-Unies ». Pour qu'il reçoive une application, il convient de caractériser une « agression armée », préambule à toute riposte se basant sur « le droit naturel de

légitime défense ». Nous sommes là, dans le champ du droit des conflits armés et non du droit pénal classique. Il est à noter que de prime abord, cette branche du droit international humanitaire n'est pas à même de recevoir application pour les attaques menées dans le cyberespace. Le groupe de travail de l'OTAN a travaillé pour justement faire entrer cette nouvelle forme de conflictualité dans le giron de cette matière. Or, si un consensus est apparu pour qualifier une cyberattaque d'agression armée, en revanche, le seuil n'est pas connu ainsi que la nature de la riposte. De ce fait, les affirmations américaines sont plus que douteuses et ne peuvent s'apparenter qu'à des démonstrations de force.

Dans le contexte actuel d'attaques informatiques sur des sites gouvernementaux ou de grandes entreprises nationales se pose la question de la riposte. La démarche de LID consiste à définir la posture à tenir face à une attaque. Déjà opérationnel, le CALID (Centre d'analyse de lutte informatique défensive) assure des missions de veille, d'analyse et d'alerte pour le ministère de la Défense. Pour sa part, la LIO consiste à « disposer d'une capacité de neutralisation à l'intérieur même des centres d'opérations adverses ».

Dans l'hypothèse d'une telle approche, l'état devrait alors utiliser des armes immatérielles offensives pour mener à bien sa riposte. Dès lors, il est nécessaire que ces armes soient catégorisées dans la classification des armes.

Devant ce vide juridique, il serait bon de proposer une définition de l'arme immatérielle dans une loi qui serait incorporée à l'article 132-75 du Code pénal dans un alinéa 3. Elle pourrait également faire l'objet d'une codification dans le Code de la défense.

Elle pourrait être rédigée de la façon suivante : « est une arme immatérielle tout logiciel ou code informatique dès lors qu'il est utilisé pour tuer, blesser, nuire à l'intégrité et la confidentialité des systèmes d'informations, structures, personnes physiques ou morales. Sera assimilé à une arme immatérielle tout maliciel utilisé ou conçu afin de présenter un risque ou une menace pour les personnes physiques, morales et les systèmes d'information ».

BIBLIOGRAPHIE

ANSSI, «L'hygiène informatique en entreprise,» ANSSI, 2012.

BORGEN C., « "Harold Koh on International Law in Cyberspace", Opinio Juris », 18 September 2012. [En ligne]. Available: http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/?utm_source=rss&utm_medium=rss&utm_campaign=harold-koh-on-international-law-in-cyberspace#sthash.VglFSW6m.dpuf.

Conseil de l'Union Européenne, « Règlement (CE) N° 428/2009 du Conseil instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage », Journal officiel de l'Union européenne, 5 mai 2009.

Direction générale des douanes et droits indirects, « Guide sur les exportations de biens et technologies à double usage », MINEFI, 2010.

FREYSSINET E., *La cybercriminalité en mouvement*, Hermes-Lavoisier, 2012.

GUILLANEUF J., « La cybercriminalité et les infractions liées à l'utilisation frauduleuse d'internet : éléments de mesure et d'analyse », INHESJ/ONDRP, 2012.

« Loi n° 2012-304 du 6 mars 2012 relative à l'établissement d'un contrôle des armes modernes, simplifié et préventif », *Journal officiel de la république française*, vol. NOR: IOCX1104583L, JORF du 7 mars 2012.

Ministère de la Défense, *Livre Blanc Défense et Sécurité Nationale*, Direction de l'information légale et administrative, Paris, 2013.

PAGET F., Secrétaire Général du CLUSIF, « Le panorama de la cybercriminalité en 2011 », INHESJ/ONDRP, 2012.

Premier Ministre, « Feuille de route du Gouvernement sur le numérique » Paris, 2013.

RAUFER X., « Retour au fondamentaux », *Le Nouvel économiste*, 10 Janvier 2013.

RID T. et MCBURNEY P., « Cyber-Weapons », *The RUSI Journal, 157:1*, p. 6-13, 2012.