Observatoire du Monde Cybernétique
Trimestriel

Juin 2013

DELEGATION AUX AFFAIRES STRATEGIQUES
MINISTERE DE LA DEFENSE

La Délégation aux Affaires Stratégiques propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation.

Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

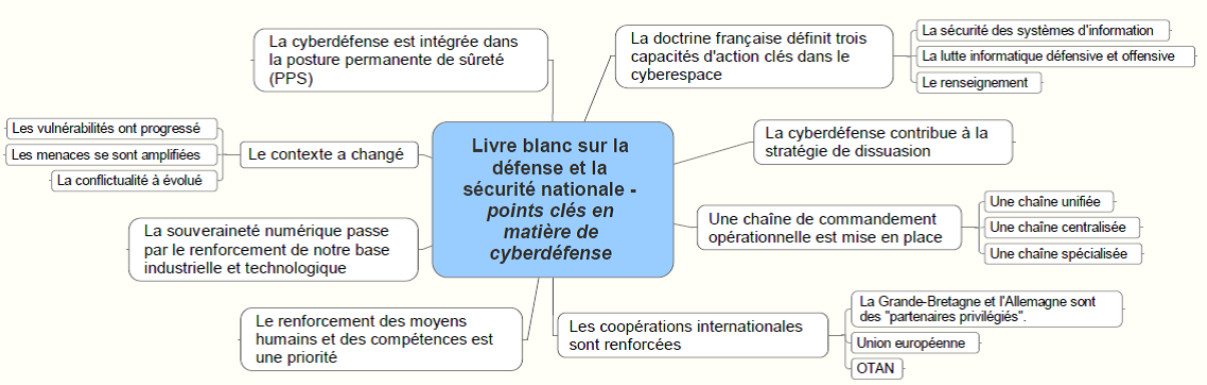
A ce titre, la DAS a confié à la **Compagnie Européenne d'Intelligence Stratégique (CEIS)** cet Observatoire du Monde Cybernétique, sous le numéro de marché 1502492543.

Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Sommaire

1. Cyberdéfense : les 10 points clés du Livre blanc sur la défense et la sécurité nationale[1]

Le Livre blanc sur la défense et la sécurité nationale de 2013 érige la cyberdéfense au rang de priorité nationale. Quelles sont les nouveautés par rapport au Livre blanc de 2008 qui évoquait pour la première fois les capacités de lutte informatique ? Quelles sont les suites de ce document à court et moyen terme ?



1.1 1er point clé : les vulnérabilités ont progressé

> *« Les systèmes d'information et leur mise en réseau sont désormais une donnée constitutive de nos sociétés. (…) Les menaces et les risques induits par l'ouverture généralisée du cyberespace ont été confirmés, qu'il s'agisse d'atteintes à des systèmes résultant d'actes hostiles intentionnels ou de ruptures accidentelles mettant en cause le fonctionnement d'une infrastructure numérique critique ».*

Les infrastructures informatiques se sont généralisées et complexifiées. Elles irriguent désormais l'ensemble des secteurs et des activités humaines, au point que nous en sommes de plus en plus dépendants. Or ce phénomène ne s'est pas accompagné d'un effort parallèle de sécurisation. L'un des points critiques concerne ainsi les systèmes assurant l'interface avec le monde physique, qu'il s'agisse des systèmes contrôlant les automatismes industriels (SCADAS), de la domotique ou des objets connectés.

[1] http://www.defense.gouv.fr/actualites/articles/livre-blanc-2013

1.2 2ème point clé : les menaces se sont amplifiées

« Les menaces militaires sont aujourd'hui un défi moins immédiat que par le passé, mais elles n'ont pas disparu. La croissance rapide des budgets de défense dans nombre de pays, en particulier en Asie, atteste leur réalité. (…) Dans le même temps, les risques et les menaces auxquels la Nation doit faire face se sont multipliés en se diversifiant. Le terrorisme, la cybermenace, le crime organisé, la dissémination des armes conventionnelles, la prolifération des armes de destruction massive, les risques de pandémies, les risques technologiques et naturels peuvent affecter gravement la sécurité de la Nation. »

Les cybermenaces figurent dans le top 3 des menaces après l'agression d'un autre Etat et le terrorisme. La menace est en fait double : la cybercriminalité mais aussi les menaces susceptibles d'affecter la sécurité nationale. Le Livre blanc adopte ainsi une vision équilibrée, réaliste et précise de la menace.

- **Une vision équilibrée**, car elle englobe à la fois la cybercriminalité cupide, mais aussi le sabotage et l'espionnage, perçu comme une menace pour l'économie et l'emploi. Ces menaces sont encore aggravées par la mondialisation et l'explosion des échanges, à l'image des flux maritimes et des problèmes de piraterie dans certaines régions.

- **Une vision réaliste**, puisqu'elle tranche avec la vision américaine basée sur la crainte d'un « Pearl harbor » informatique. Une attaque informatique majeure visant par exemple des infrastructures vitales n'est pas exclue mais la dimension asymétrique de la menace est relativisée : si certaines agressions sont relativement faciles et peu onéreuses à mettre en œuvre, les attaques sophistiquées sont particulièrement complexes.

- **Une vision précise** car plusieurs scénarios sont décrits : le vol d'informations personnelles à des fins de chantage, les tentatives de pénétration de réseaux numériques à des fins d'espionnage, la destruction ou la prise de contrôle à distance de systèmes informatisés contrôlant des activités critiques, comme des systèmes d'armes ou des capacités militaires stratégiques. Qui plus est, il est clairement indiqué que la menace peut venir d'Etats développant des capacités informatiques offensives. La Chine, laquelle a poursuivi le développement et la modernisation de « *son arsenal nucléaire et de ses capacités de projection de puissance et de cyberattaques »* est même explicitement citée.

1.3 3ème point clé : la conflictualité a évolué

« Il est vraisemblable que les opérations aéro-maritimes et les actions indirectes seront préférées à des campagnes aéroterrestres lourdes et de longue durée. Les opérations ciblées conduites par les forces spéciales et les frappes à distance, qu'elles soient cinétiques ou cybernétiques, devraient devenir plus fréquentes, compte tenu de leur souplesse d'emploi dans un contexte où les interventions classiques continueront d'être politiquement plus difficiles et parfois moins efficaces. »

Le cyberespace est considéré comme le 5ème espace de bataille et un champ de confrontation à part entière. Il ne s'agit donc plus d'agir dans ce milieu uniquement de façon subie, mais également de façon opportuniste lorsque l'analyse démontre que les effets recherchés peuvent être atteints via des capacités cybernétiques. Compte tenu de leur souplesse d'emploi, les frappes à distance cybernétiques, de même que les opérations ciblées menées par des forces spéciales, sont donc considérées comme des options valables dans un contexte où « *les interventions classiques continueront d'être politiquement plus difficiles et parfois moins efficaces* ».

Ce changement majeur transparait aussi des propos de Jean-Yves Le Drian lors d'un colloque organisé par l'Ecole des transmissions de Rennes en juin 2013 : « *la capacité offensive enrichit la palette des options qui sont à la disposition de l'état. (…) Le concept de cyberattaque ne nous est plus étranger*[2] ». Là aussi, l'approche est se veut réaliste : les actions de coercition dans un contexte de haute intensité ne sont pas écartées, les capacités « cyber » n'étant qu'une option parmi d'autres.

1.4 4ème point clé : la cyberdéfense est intégrée dans la posture permanente de sûreté

« Ainsi, l'échelle des priorités qui détermine le niveau et l'intensité de nos engagements potentiels, s'ordonne comme suit : protéger le territoire national et les ressortissants français, et garantir la continuité des fonctions essentielles de la Nation ; garantir ensemble la sécurité de l'Europe et de l'espace nord-atlantique ; stabiliser ensemble les approches de l'Europe ; participer à la stabilité du Proche-Orient et du golfe arabo-persique ; contribuer à la paix dans le monde. »

[2] http://www.rpfrance-otan.org/IMG/pdf/Discours_cyber_ETRS-1.pdf

Le dispositif de cyberdéfense complète la posture permanente de sûreté avec pour priorités stratégiques :

- La protection du territoire et des ressortissants face à des cyberattaques, qu'il s'agisse d'action cybercriminelles, de sabotage ou d'espionnage affectant le potentiel scientifique, technique et industriel de la Nation ;

- La garantie de la sécurité de l'Europe et de l'espace nord-Atlantique. On retrouve ici l'idée d'une sécurité collective dans le cyberespace à travers un ensemble de coopérations bilatérales ou multilatérales ;

- La participation à la stabilité du Proche-Orient et du Golfe arabo-persique. Au plan informatique, cette région revêt une importance particulière : plusieurs Etats de la zone, qu'il s'agisse d'Israël ou de l'Iran, ont développé des capacités de lutte informatique ; d'autres comme l'Arabie saoudite ou le Qatar ont fait l'objet d'attaques récentes.

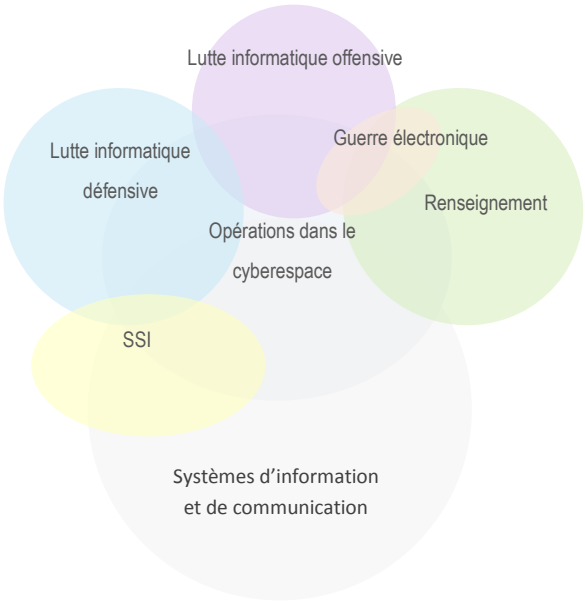
1.5 5ème point clé : la doctrine française définit trois capacités d'action clés dans le cyberespace

Trois capacités d'actions essentielles dans le cyberespace sont identifiées :

- **La sécurité des systèmes d'information.** Elle permet d'assurer la protection et la résilience des systèmes d'information de l'Etat, des opérateurs d'infrastructures vitales (OIV) et des industries stratégiques. Dans la pratique, une directive sur la sécurité des réseaux et de l'information (SRI) a été proposée en février 2013 pour élever le niveau de sécurité des réseaux européens et rendre obligatoire les notifications d'incidents aux autorités compétentes. Cette directive se traduira en France par un nouveau dispositif réglementaire applicable aux OIV sur lequel travaille l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et qui devrait être intégré à la rentrée dans la Loi de programmation militaire (LPM).

- **La lutte informatique, à la fois défensive et offensive.** Cette dernière soulève un débat juridique qui suppose selon le Livre blanc « une réflexion internationale ». De fait, la question de la compatibilité de la lutte informatique avec le droit international est délicate, dès lors que l'on se situerait dans une attaque informatique susceptible de parvenir au niveau de force requis pour être qualifiée d'agression armée. Faut-il baisser ce niveau pour englober des attaques informatiques qui n'atteindraient pas ce seuil aujourd'hui et permettre ainsi l'exercice de la légitime défense, quitte à multiplier les risques d'escalade ? Faut-il introduire une nouvelle forme d'agression informatique ? Faut-il maintenir une zone d'incertitude quant à ce seuil, ce qui peut contribuer à la dissuasion ? Autant de questions traitées par le groupe d'experts mis en place par le Centre d'excellence de cyberdéfense de l'OTAN à Tallinn (CCDCOE) auquel la France a adhéré en 2012 et auprès duquel elle détachera un personnel du Ministère de la défense à compter de l'été 2013.

- **Le renseignement.** Le cyberespace constitue à travers sa couche cognitive un terrain privilégié pour des opérations de renseignement, qu'il s'agisse de sources ouvertes (le Livre blanc insiste sur le besoin de disposer d'outils spécifiques d'analyse des sources multimédias) ou d'actions clandestines. Mais il est aussi en tant que tel, et en raison du « brouillard » qui le caractérise, l'objet d'actions de renseignement visant à évaluer les dispositifs adverses, détecter les attaques le plus en amont possible et identifier leur origine.



1.6 6ème point clé : la cyberdéfense contribue à la stratégie de dissuasion

> [la doctrine nationale de réponse aux agressions informatiques majeures repose sur] *une capacité de réponse gouvernementale globale et ajustée face à des agressions de nature et d'ampleur variées faisant en premier lieu appel à l'ensemble des moyens diplomatiques, juridiques ou policiers, sans s'interdire l'emploi gradué de moyens relevant du ministère de la défense, si les intérêts stratégiques nationaux étaient menacés.*

La posture de cyberdéfense, à travers les trois capacités décrites plus haut, contribue à la stratégie de dissuasion qui est appréhendée de façon globale. La résilience à elle seule ne peut en effet dissuader un éventuel attaquant. Par ailleurs, la réponse à une attaque informatique n'est ni forcément symétrique ni systématiquement dans le cyberespace. Sans envisager une éventuelle riposte nucléaire face à une attaque informatique massive comme dans la doctrine américaine, il est envisagé de répondre de façon graduelle à travers des moyens diplomatiques, juridiques, policiers, voire militaires, dès lors qu'on admet qu'une attaque de grande envergure est susceptible d'être un véritable acte de guerre et d'entraîner des destructions matérielles et des pertes en vies humaines. La prochaine Loi de programmation militaire devrait par ailleurs comprendre des dispositions

permettant sous certaines conditions aux défenseurs de remonter jusqu'aux attaquants, où qu'ils se trouvent.

1.7 7ème point clé : une chaîne de commandement « cyber » unifiée, centralisée et spécialisée

« L'organisation opérationnelle des armées intégrera ainsi une chaîne opérationnelle de cyberdéfense, cohérente avec l'organisation et la structure opérationnelles de nos armées, et adaptée aux caractéristiques propres à cet espace de confrontation : unifiée pour tenir compte de l'affaiblissement de la notion de frontière dans cet espace ; centralisée à partir du centre de planification et de conduite des opérations de l'état-major des armées, pour garantir une vision globale d'entrée et une mobilisation rapide des moyens nécessaires ; et spécialisée car demandant des compétences et des comportements adaptés. »

Comme pour les autres environnements, le cyberespace dispose désormais d'une chaîne de commandement opérationnelle qui est déployée depuis juin 2011 et est actuellement en phase de montée en puissance. Comme l'a souligné le Ministre à Rennes le 3 juin dernier, il s'agit « d'offrir une vision globale et une mobilisation rapide des moyens en cas de besoin, tout en s'intégrant pleinement aux autres chaines de conduite des opérations maritimes, aériennes, terrestre ou spéciales. Car il ne s'agit pas de greffer un nouveau service qui serait autonome, mais au contraire d'irriguer, sous un commandement unifié, l'ensemble des actions menées. » L'organisation prend ainsi en compte la transversalité du cyberespace par rapport aux autres milieux. Pour tenir compte de la spécificité de ce milieu, l'objectif est également de privilégier les boucles courtes et de mutualiser les équipements et les moyens. Dans cette logique, le centre de surveillance de l'ANSSI et le Centre d'Analyse et de Lutte Informatique défensive (CALID) du Ministère de la défense seront prochainement colocalisés dans un immeuble parisien. La DGA-Maîtrise de l'information s'est enfin vue confiée le pilier technologique, qu'il s'agisse d'analyse de la menace, d'expertise technique ou de recherche amont.

1.8 8ème point clé : les coopérations internationales seront renforcées

« Toute politique ambitieuse de cyberdéfense passe par le développement de relations étroites entre partenaires internationaux de confiance. Les relations seront approfondies avec nos partenaires privilégiés, au premier rang desquels se placent le Royaume-Uni et l'Allemagne. Au niveau européen, la France soutient la mise en place d'une politique européenne de renforcement de la protection contre le risque cyber des infrastructures vitales et des réseaux de communications électroniques. »

La puissance dans le cyberespace ne s'évalue pas qu'en termes de ressources, qu'il s'agisse d'infrastructures, de capacités scientifiques ou techniques ou de la base industrielle et technologique. En raison du caractère transnational du cyberespace, elle est aussi fonction de la capacité des Etats à rayonner (pouvoir d'attraction) et à nouer des coopérations. Plusieurs cercles concentriques se dessinent ainsi : le Royaume-Uni et l'Allemagne, qui sont pour la première fois nommément désignés comme les partenaires privilégiés, l'Union européenne, qui a adopté en février 2013 sa stratégie pour un « cyberespace ouvert, sûr et sécurisé » et enfin l'OTAN, qui a élaboré une politique de cyberdéfense en juin 2011. Les lignes de partage entre le périmètre de souveraineté nationale et ce qui peut être partagé dans le cadre d'une coopération, de même qu'entre les rôles respectifs de l'Union européenne et de l'OTAN restent cependant à préciser. Ce sera l'une des questions abordée lors du Conseil européen de décembre prochain qui sera consacré aux questions de défense.

1.9 9ème point clé : la souveraineté numérique passe par le renforcement de notre base industrielle et technologique

« La capacité à produire en toute autonomie nos dispositifs de sécurité, notamment en matière de cryptologie et de détection d'attaque, est à cet égard une composante essentielle de la souveraineté nationale. Un effort budgétaire annuel en faveur de l'investissement permettra la conception et le développement de produits de sécurité maîtrisés. Une attention particulière sera portée à la sécurité des réseaux de communication électroniques et aux équipements qui les composent. Le maintien d'une industrie européenne performante en la matière est un objectif essentiel. »

La maîtrise de certaines technologies et infrastructures clés est un élément essentiel de la souveraineté numérique. Alors que l'Europe a été récemment qualifiée de « nouvelle colonie du monde numérique » dans un rapport du Sénat[3], la priorité est donc donnée au renforcement de la base industrielle et technologique en matière de sécurité. Au plan européen, l'objectif est ainsi de développer un marché numérique unique et d'utiliser l'ensemble des leviers (politique de la concurrence, soutien à l'innovation, politique d'achat public…) de la politique industrielle. Au niveau national, une politique industrielle volontariste est en cours d'élaboration. Des actions concrètes ont par exemple été lancées pour renforcer les crédits consacrés aux études amont et à la R&D.

[3] http://www.senat.fr/notice-rapport/2012/r12-443-notice.html

1.10 10ème point clé : le renforcement des moyens humains et des compétences est une priorité

« Il y a aujourd'hui une urgence nationale à augmenter de manière très significative le niveau de sécurité et les moyens de défense de nos systèmes d'information, tant pour le maintien de notre souveraineté que pour la défense de notre économie et de l'emploi en France. Les moyens humains qui y sont consacrés seront donc sensiblement renforcés, à la hauteur des efforts consentis par nos partenaires britannique et allemand. »

Le développement de la base industrielle et technologique suppose le renforcement des moyens humains et des compétences, tant sur un plan quantitatif que qualitatif. Après la création d'une réserve citoyenne dédiée à la cyberdéfense, le Livre blanc annonce ainsi la création prochaine d'une réserve opérationnelle spécialisée. Dans cette optique, le Ministère de la défense a ainsi annoncé la création d'un pôle de cyberdéfense associant les compétences des armées et de la DGA, celles des Ecoles de Saint-Cyr-Coetquidan, des universités et écoles d'ingénieur situées en Bretagne.

Le Livre blanc de 2013 marque donc une nouvelle étape dans le développement du dispositif de cyberdéfense français. La loi de programmation militaire qui sera promulguée à la rentrée prochaine devra maintenant traduire dans les faits les priorités annoncées.

2. Le cadre juridique français de la rétro-ingénierie et des tests d'intrusion

Sous-titre 1. Le régime juridique de la rétro-ingénierie informatique

1.0 Chapitre préliminaire : Définition et cadres d'emploi de la rétro-ingénierie informatique

1.0.1 Définition

L'ingénierie inverse, rétro-conception ou « reverse engineering » est l'*« activité qui consiste à étudier un objet pour en déterminer le fonctionnement interne ou la méthode de fabrication »*[45]. Ainsi, grâce aux méthodes de rétro-conception, il est possible de comprendre le comportement du logiciel, sans en détenir ni le code source ni la documentation[6].

1.0.2 Focus sur les différents modes de rétro-conception.

Cette analyse se réalise en général sur un ordinateur déconnecté du réseau ou sur une machine virtuelle, grâce à des outils tels que des désassembleurs[7], débogueurs[8] ou décompilateurs[9]. Elle peut être « statique » (analyse des différents composants du logiciel) ou « dynamique » (observation du comportement du logiciel, en cours d'exécution). Lors de l'analyse, le rétro-ingénieur se pose les questions suivantes : quel type de menace représente ce logiciel ? Comment se propage-t-elle ? Quelles actions lance-t-elle ? Quelles informations cible-t-elle ? En somme, quelle est sa finalité et comment m'en défendre ?

---

[4] Wikipedia - https://fr.wikipedia.org/wiki/R%C3%A9troing%C3%A9nierie
[5] http://www.labri.fr/perso/tabary/cours/0910/secu_lp/cours5.pdf
[6] http://www.quarkslab.com/fr-services#reverse
[7] Permet, à partir d'un exécutable, d'obtenir son code en langage machine - http://www.labri.fr/perso/tabary/cours/0910/secu_lp/cours5.pdf
[8] « Permet de suivre le déroulement d'un programme pas à pas, de contrôler son exécution. Plus intrusif qu'un désassembleur, le débogueur permet de mieux analyser le programme « en cours d'exécution » - http://www.labri.fr/perso/tabary/cours/0910/secu_lp/cours5.pdf
[9] « Outil servant à reconstituer, partiellement ou totalement, le code source d'un logiciel à partir d'un programme exécutable alors dans un format binaire » - Wikipedia

1.0.3 Cadre d'emploi : un usage dual en sécurité informatique

1.0.3.1 L'usage défensif et préventif

Dans un contexte de cyberdéfense, la rétro-conception de logiciels peut être utile à plusieurs fins. La première sera d'étudier le virus, le ver ou le rootkit[10] pour **améliorer les outils de détection** et de défense. Le rétro-ingénieur pourra ainsi analyser la réelle capacité de nuisance du logiciel malveillant[11], et générer une signature afin de lutter contre une « nouvelle menace à propagation rapide ». C'est d'ailleurs le moyen le plus courant d'analyse, pratiqué par de nombreux éditeurs de solutions de sécurité pour décrypter les nouvelles menaces. Le « mouchard » développé par les autorités allemandes, similaire à celui autorisé en France par la LOPSSI 2, en a d'ailleurs été l'objet. Dans un article datant du 10 août 2011, le Chaos Computer Club[12] met à nu ce « mouchard » ayant pourtant comme finalité de rester discret.[13]

La seconde des finalités de la rétro-ingénierie de logiciels sera la recherche de vulnérabilités, comme des failles Zero-day, réalisée par une entreprise mandatée, ou par l'éditeur lui-même, sur ses propres logiciels. Il s'agit là d'une activité courante pour les entreprises agrémentées ou pour les éditeurs souhaitant évaluer le niveau de sécurité de leurs applications[14].

Exemple : à la suite d'une attaque informatique, l'ingénierie inversée permettra de comprendre comment l'attaque s'est déroulée, si l'attaque est toujours en cours et ce qui a potentiellement été perdu ou endommagé lors de cette attaque.[15] Il sera ici possible de faire la réelle distinction entre un programme inoffensif et intrusif (du spam) et un réel virus de type keylogger ou autre. Il sera également intéressant d'identifier quels types d'informations l'attaque cherche à récupérer. Cette démarche semble très constructive et complémentaire de la mise en place de SOC et de l'analyse et la corrélation de logs à travers les méthodes SIEM.[16]

1.0.3.2 L'usage offensif

Le rétro-ingénieur pourra étudier le code d'une attaque informatique pour le reproduire, voire l'améliorer à des fins de riposte, ou tout simplement se l'approprier et bénéficier, sans supporter de

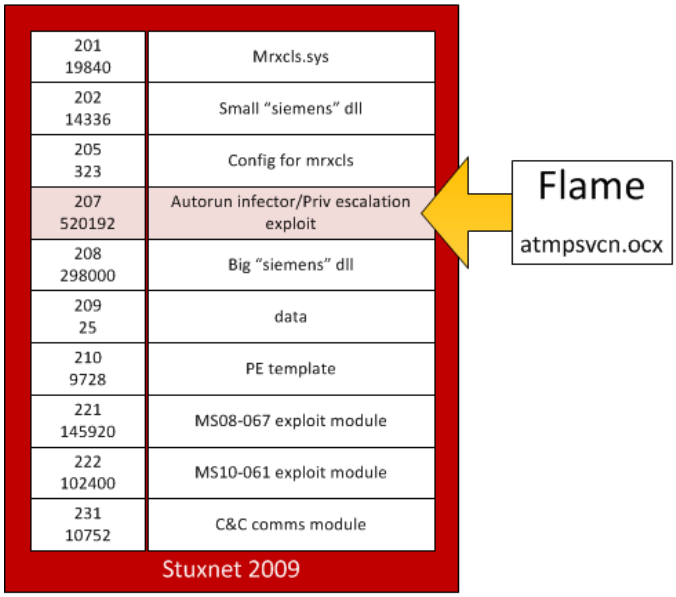
[10] Variété de malware ; « ensemble de techniques mises en œuvre par un ou plusieurs logiciels, dont le but est d'obtenir et de pérenniser un accès (généralement non autorisé) à un ordinateur de la manière la plus furtive possible » - http://searchmidmarketsecurity.techtarget.com/definition/rootkit
[11] http://magazine.qualys.fr/produits-technologies/le-reverse-engineering-ou-retro-ingenierie-explique/
[12] « Analysis of the government malware » (PDF, Allemand) - http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf
[13] http://www.ccc.de/en/updates/2011/staatstrojaner
[14] http://www.labri.fr/perso/tabary/cours/0910/secu_lp/cours5.pdf
[15] http://www.itworld.com/security/342999/security-beauty-malware-reverse-engineering
[16] Voir également : www.cert.org/archive/pdf/malware-7-07.pdf - CERT, « The Use of Malware Analysis in Support of Law Enforcement »

coûts de R&D, d'armes informatiques redoutables, mais incontrôlables une fois diffusées sur Internet[17]. On parle alors de « malware re-engineering »[18].

Mais c'est aussi une technique privilégiée par les pirates informatiques à la recherche de nouvelles vulnérabilités dans les applications et les systèmes d'exploitation ciblés. La rétro-conception peut donc servir :

- à de l'espionnage industriel ;
- au piratage de logiciel protégé par les droits d'auteurs (ou « cracking ») ;
- à la recherche de vulnérabilité pour une exploitation ou diffusion à des personnes mal intentionnées.

Exemple : suite à la diffusion accidentelle du vers Stuxnet sur le réseau mondial, nombreux sont les Etats et autres entités à avoir pu récupérer cette arme informatique sans précédent, pour l'améliorer, à des fins de nouvelles cyberattaques. Des « modules » ou tranches de code peuvent être réexploités afin de réaliser un nouveau programme malveillant. C'est d'ailleurs ce qu'a réussi à prouver l'équipe de Kaspersky Lab et révélant les liens entre Flame et Stuxnet.



« Map of resources in Stuxnet 2009 »[19]

[17] Ce cas de figure soulève des problématiques similaires à celles relatives aux armements plus classiques, et à la prolifération incontrôlée d'outils nocifs.
[18] http://cs.gmu.edu/~astavrou/courses/ISA_785_F11/Malware%20Reverse%20Engineering%20(Class).pdf
[19] http://www.securelist.com/en/blog/208193568/Back_to_Stuxnet_the_missing_link#page_top

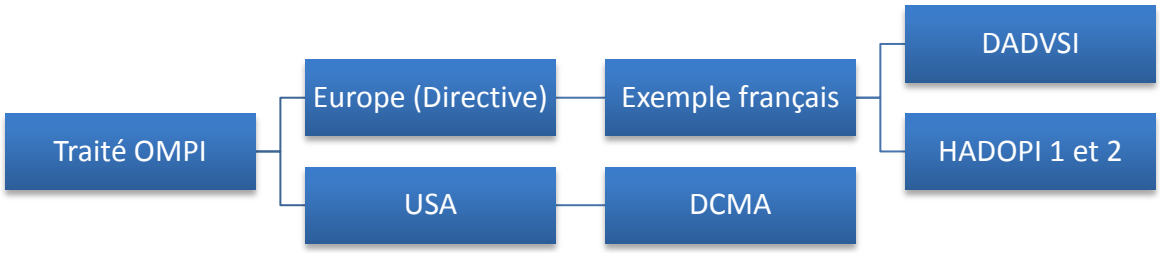
De ces éléments de définition apparaissent deux cas de figure au traitement juridique distinct : la rétro-ingénierie de logiciel informatique « légitime » et la rétro-ingénierie de logiciel informatique « malveillant ». Si la rétro-ingénierie de logiciel informatique est principalement encadrée par la protection de la propriété intellectuelle et les stipulations contractuelles, l'analyse de malware est, elle, confrontée à d'autres considérations juridiques.

1.1 Chapitre 1. La rétro-ingénierie de programmes informatiques

1.1.1 L'ingénierie inversée face à la protection de la propriété intellectuelle

1.1.1.1 La superposition du contrat et des lois nationales

Si les éditeurs sont nombreux à interdire ou limiter l'ingénierie inversée de leurs logiciels dans leurs conditions d'utilisation, l'ingénierie inverse reste une pratique légale dans de nombreux pays, bien qu'encadrée. Elle est notamment autorisée à des fins de d'interopérabilité. Et dans les pays où cette pratique est autorisée, les clauses ne sont pas valables, ou le sont dans les limites définies par la loi. Enfin, l'ingénierie inversée est gouvernée par le droit de la propriété intellectuelle, droit propre à chaque Etat. Il en découle une relative insécurité juridique pour les prestataires de services ou les chercheurs.



« Le premier pas fut le traité de l'Organisation Mondiale de la Propriété Intellectuelle (OMPI) en 1996, qui fut appliqué aux Etats-Unis, à travers le Digital Millenium Copyright Act (DMCA) en 1998, en Europe par le biais de la directive sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (2001/29/EC), et en France, avec tout d'abord la loi sur les Droits d'Auteurs et Droits Voisins dans la Société de l'Information (DADVSI) en 2006, puis la loi Création et Internet, connue aussi sous le nom de loi HADOPI en référence à la Haute Autorité qu'elle met en place, en juin 2009, et la loi HADOPI 2 en septembre 2009. »[20]

[20] http://m2bde.u-paris10.fr/content/les-dispositions-l%C3%A9gales-contre-le-contournement-des-mesures-techniques-pour-la-protection-d

1.1.1.2 Le régime juridique français

C'est l'article L 122-6-1 du code de la propriété intellectuelle français qui autorise le reverse engineering. Mais cette autorisation est strictement encadrée.

Le principe est celui du droit de propriété exclusif et opposable de l'auteur du logiciel, droit concédé partiellement aux « clients » ou « acheteurs » par le biais de licences d'utilisation, par exemple. L'article 122-6-1 qui autorise l'ingénierie inversée constitue une exception à ce système. Exception envisagée dans deux cas de figure : le premier est l'exigence d'interopérabilité, le second l'utilisation conforme à la destination du logiciel.

Extraits de l'article L122-6-1 : le reverse engineering autorisé à des fins d'interopérabilité

« III. La personne ayant le droit d'utiliser le logiciel peut sans l'autorisation de l'auteur *observer, étudier ou tester le fonctionnement de ce logiciel* afin de déterminer les idées et principes qui sont à la base de n'importe quel élément du logiciel lorsqu'elle effectue toute opération de chargement, d'affichage, d'exécution, de transmission ou de stockage du logiciel qu'elle est en droit d'effectuer. »

« IV. La reproduction du code du logiciel ou la traduction de la forme de ce code n'est pas soumise à l'autorisation de l'auteur lorsque la reproduction ou la traduction au sens du 1° ou du 2° de l'article L. 122-6[21] est indispensable pour obtenir les informations nécessaires à l'interopérabilité d'un logiciel créé de façon indépendante avec d'autres logiciels, sous réserve que soient réunies les conditions suivantes :

- 1° Ces actes sont accomplis par la personne ayant le droit d'utiliser un exemplaire du logiciel ou pour son compte par une personne habilitée à cette fin ;
- 2° Les informations nécessaires à l'interopérabilité n'ont pas déjà été rendues facilement et rapidement accessibles aux personnes mentionnées au 1° ci-dessus ;
- 3° Et ces actes sont limités aux parties du logiciel d'origine nécessaires à cette interopérabilité.

Les informations ainsi obtenues ne peuvent être :

- 1° Ni utilisées à des fins autres que la réalisation de l'interopérabilité du logiciel créé de façon indépendante ;
- 2° Ni communiquées à des tiers sauf si cela est nécessaire à l'interopérabilité du logiciel créé de façon indépendante ;

[21] **Article L122-6 – Code de la propriété intellectuelle français**
« Sous réserve des dispositions de l'article L. 122-6-1, le droit d'exploitation appartenant à l'auteur d'un logiciel comprend le droit d'effectuer et d'autoriser :
1° La reproduction permanente ou provisoire d'un logiciel en tout ou partie par tout moyen et sous toute forme. Dans la mesure où le chargement, l'affichage, l'exécution, la transmission ou le stockage de ce logiciel nécessitent une reproduction, ces actes ne sont possibles qu'avec l'autorisation de l'auteur ;
2° La traduction, l'adaptation, l'arrangement ou toute autre modification d'un logiciel et la reproduction du logiciel en résultant ;
3° La mise sur le marché à titre onéreux ou gratuit, y compris la location, du ou des exemplaires d'un logiciel par tout procédé. Toutefois, la première vente d'un exemplaire d'un logiciel dans le territoire d'un Etat membre de la Communauté européenne ou d'un Etat partie à l'accord sur l'Espace économique européen par l'auteur ou avec son consentement épuise le droit de mise sur le marché de cet exemplaire dans tous les Etats membres à l'exception du droit d'autoriser la location ultérieure d'un exemplaire. »

- 3° Ni utilisées pour la mise au point, la production ou la commercialisation d'un logiciel dont l'expression est substantiellement similaire ou pour tout autre acte portant atteinte au droit d'auteur. »

« V. Le présent article ne saurait être interprété comme permettant de porter atteinte à l'exploitation normale du logiciel ou de causer un préjudice injustifié aux intérêts légitimes de l'auteur. »

Toute stipulation contraire aux dispositions prévues aux II, III et IV du présent article est nulle et non avenue.

1.1.1.2.1 L'interopérabilité

Le reverse engineering d'un logiciel à des fins d'interopérabilité permet, grâce à une technique de décompilation, d'autoriser le logiciel à « échanger des informations » et « utiliser mutuellement des informations » avec d'autres logiciels.[22] Souvent indispensable pour la création d'outil compatibles avec certains logiciels ou terminaux, le reverse engineering reste encadré à des fins de protection de la propriété intellectuelle. L'objectif étant d'exclure tout espionnage industriel, copie, ou contournement de mesures de sécurité. Pour ce faire, trois conditions sont à respecter :

- Que les informations permettant l'interopérabilité ne soient accessibles par aucun autre moyen ;
- Que le reverse engineering ne soit exercé que par l'utilisateur légitime du logiciel ;
- Que le reverse engineering ne concerne que les parties du logiciel directement concernées par l'interopérabilité.

C'est le contrat qui définira la finalité, la « destination » du logiciel. Ce système est également celui proposé par le droit finlandais.

1.1.1.2.2 Le contournement des mesures de protection

Le reverse engineering ne doit pas « porter atteinte sciemment, à des fins autres que la recherche [aux mesures de protection du droit d'auteur] »[23].

1.1.1.3 Les Etats-Unis[24]

1.1.1.3.1 Le principe du DCMA[25]

Adopté en 1998, le Digital Millenium Copyright Act (DCMA), loi de lutte contre le piratage, envisage la possibilité d'interdire le contournement de technologies de protection des droits d'auteur.

---

[22] Cette définition de l'interopérabilité est proposée par la Directive 91/250/CEE du Conseil, du 14 mai 1991, concernant la protection juridique des programmes d'ordinateur - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991L0250:FR:HTML

[23] DADVSI, art. 13 et 22.

[24] https://www.eff.org/issues/coders/reverse-engineering-faq#faq1

[25] D'autres textes sont concernés : la « Copyright law and fair use » (17 U.S.C. 107) ; Le « Electronic Communications Privacy Act », (18 U.S.C. 2510 et. Seq) ; Trade Secret Law.

1.1.1.3.2 Le cas Lexmark : l'interopérabilité est un « fair use »[26]

Dans une affaire datant de décembre 2002, la cour a cependant admis que le reverse engineering à des fins d'interopérabilité était parfaitement légal et éthique. [27] Il est depuis lors soutenu que le DCMA ne s'oppose pas au reverse engineering à des fins d'interopérabilité.

1.1.1.3.3 L'importance du contrat

Le régime juridique étatsunien accorde également une place importante au contrat. A travers des End User License Agreements (EULA), terms of service notices (TOS), terms of use notices (TOU) (ou Conditions générales d'utilisation), accords de non-divulgation ou de confidentialité, mais aussi par les contrats encadrant l'usage des API ou la prestation de développement, le propriétaire du logiciel est susceptible d'encadrer la pratique du reverse engineering, notamment en définissant strictement la finalité de son logiciel.

1.1.2 Focus sur l'ingénierie inversée au service de la recherche de failles de sécurité dans un logiciel

> *« On n'a donc pas le droit en France de démontrer techniquement qu'un logiciel présente des failles de sécurité, ou que la publicité pour ces logiciels est mensongère. Dormez tranquilles, citoyens, tous vos logiciels sont parfaits. »*[28]

Cette citation du chercheur agissant sous le pseudonyme de Guillermito fait suite à sa condamnation pour avoir « reproduit, modifié, et rassemblé tout ou partie du logiciel Viguard puis procédé à la distribution gratuite de logiciels tirés des sources du logiciel Viguard »[29], en contradiction avec la licence. « Le fait que celui qui agissait sous le pseudonyme Guillermito ait commis ces actes dans le but de **détecter les failles de sécurité du logiciel Viguard** et d'en faire profiter la communauté dans les forums de discussion n'entre pas dans le cadre de [l'exception] prévue au monopole de l'auteur [prévue par l'article L122-6-1 du Code de procédure pénale]. »[30]

Le Digital Millennium Copyright Act (US Code, Title 12, section 1201(i)–(j)) autorise la recherche de failles de sécurité sur des logiciels, sous réserve qu'elle ne nuise pas aux droits de l'auteur du logiciel.[31]

En droit français, la simple recherche de failles de sécurité n'est pas réprimée en tant que telle, sous réserve de respect du régime juridique relatif au respect du droit de la propriété intellectuelle. C'est

---

[26] D'autres cas jurisprudentiels : Sega Enterprises v. Accolade (977 F.2d 1510 (9th Cir. 1992)) ; Sony Computer Entertainment v. Connectix (203 F.3d 596 (9th Cir. 2000)) ; Atari Games Corp. v. Nintendo of America, Inc. (975 F.2d 832 (Fed. Cir. 1992)) ; Compaq Computer Corp. v. Procom Technology, Inc. (908 F. Supp. 1409 (S.D. Tex. 1995)) ; Blizzard v. BnetD (Davidson & Associates DBA Blizzard Entertainment, Inc.; Vivendi Universal Inc. v. Jung et al., 422 F.3d 630 (8th Cir. 2005)).
[27] http://ethics.csc.ncsu.edu/intellectual/reverse/study.php
[28] http://www.guillermito2.net/index.html
[29] http://www.pcinpact.com/archive/26857-Affaire-Guillermito-nouvel-echec-en-appel.htm
[30] http://www.legalis.net/spip.php?page=breves-article&id_article=1659
[31] http://www.cs.columbia.edu/~angelos/Papers/2010/msp2010020067.pdf

la publication des résultats, la « démonstration technique » de ces recherches qui peut être sanctionnée par l'article 323-3-1 du Code pénal.

Full et responsible disclosure[32]

Il existe plusieurs chapelles parmi les passionnés de sécurité informatique. Certains vont informer le propriétaire du site internet, ou l'éditeur du logiciel, de l'existence de cette faille afin que ce dernier la corrige au plus vite : c'est ce qu'on appelle un « *white hat* »[33]. Parmi ceux-ci, certains sont partisans du « *full disclosure* » ou divulgation complète, alors que d'autres prônent le « *responsible disclosure* » ou divulgation responsable.

La différence entre les deux positions tient à l'étendue des informations révélées. Dans le cas de la divulgation « complète », toutes les informations connues concernant la faille sont publiées, y compris les « *exploits* », c'est-à-dire les moyens d'exploiter la faille. L'idée est que la faille sera plus rapidement prise au sérieux et corrigée si toutes les données à son sujet sont rendues publiques. Les partisans de la divulgation « responsable » choisissent de laisser un certain temps à l'intéressé pour corriger la faille, et s'ils choisissent de divulguer l'existence d'une faille, ils ne fournissent en principe pas les « *exploits* ». D'autres enfin estiment qu'effectuer une divulgation complète mais dans un cercle d'initiés restreints constitue également une « *responsible disclosure* ».

L'article 323-3-1[34] du Code pénal sanctionne *« 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 »*, c'est-à-dire le fait d'accéder, de se maintenir frauduleusement, d'entraver, de fausser le fonctionnement ou d'introduire des données dans un systèmes de traitement automatisé de données [STAD]. Ici, c'est le fait d'offrir, de céder ou de mettre à disposition qui remet en cause ces pratiques de « disclosure ».

Il est légitime d'envisager que la finalité de sécurité informatique du reverse engineering entre dans la définition du motif légitime évoqué dans l'article 323-3-1 du Code pénal. Mais ce constat amène plusieurs interrogations : Ne peut-on pas imaginer que le droit à l'information constitue un motif légitime de possession ou de diffusion d'un des outils incriminés par l'article 323-3-1 du Code pénal ? D'autre part, doit-on apprécier la « finalité de sécurité informatique » de façon directe ou indirecte ? En effet, le motif légitime ne manquera pas d'être invoqué de façon indirecte par certains « *white hat* » pour justifier des « *full disclosure* ». Leur raisonnement sera de justifier des divulgations complètes en expliquant que ces dernières placent les titulaires des droits sur les sites ou les logiciels

[32] OMC, 07/2012, Point juridique sur la publication de failles de sécurité
[33] Les « black hats » ne sont pas directement concernés par les problématiques de publication des failles. En effet, ces derniers ont tout intérêt à conserver les failles inconnues afin de pouvoir les exploiter en toute tranquillité.
[34] http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418323&cidTexte=LEGITEXT000006070719&dateTexte=20120601&oldAction=rechCodeArticle

vulnérables dos au mur, et les oblige à intervenir car la faille est accessible à n'importe quel « *script kiddies* »[35].

1.2 Chapitre 2. Le cas particulier du reverse engineering de malwares[36]

Bien évidemment, le malware n'est pas protégé[37] par la propriété intellectuelle. Son analyse ne peut donc être soumise au régime juridique décrit ci-dessus. En tant que tel, l'ingénierie inversée de malware est légale. Mais plus que le fait de procéder à une analyse du malware, c'est sa possession qui risque de tomber sous le coup de l'article 323-3-1 du Code pénal.

1.2.1 La collision avec les incertitudes de l'article 323-3-1 : la simple possession du malware analysé peut être illégale[38]

L'article 323-3-1[39] du Code pénal sanctionne *« 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 »*, c'est-à-dire le fait d'accéder, de se maintenir frauduleusement, d'entraver, de fausser le fonctionnement ou d'introduire des données dans un systèmes de traitement automatisé de données [STAD]. Ce comportement « *est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée* », c'est-à-dire au maximum 7 ans de prison et 100 000€ d'amende.

Cette transposition de l'article 6[40] de la Convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001 par la Loi pour la Confiance dans l'Economie Numérique (LCEN) du 21 juin 2004 a pour finalité de sanctionner la production et la détention de virus informatiques[41].

---

[35] http://fr.wikipedia.org/wiki/Script_kiddie
[36] Les incertitudes juridiques de la publication de failles de sécurité, CEIS - http://fic2013.com/les-incertitudes-juridiques-de-la-publication-de-failles-de-securite/
[37] http://www.bankofmalware.com/isitlegal.php
[38] Pour en savoir plus, voir : Lettre Mensuelle de l'OMC n°07 – Juillet 2012, « Point juridique sur la publication de failles de sécurité »
[39]http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418323&cidTexte=LEGITEXT000006070719&dateTexte=20120601&oldAction=rechCodeArticle
[40] Article 6 – Abus de dispositifs
1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:
a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:
i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;
ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique,
dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et
b la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.
2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du

1.2.1.1 Le malware analysé est un outil « conçu ou spécialement adapté » pour commettre des atteintes au STAD

L'article a une portée relativement large. Et difficile de cerner clairement quels outils informatiques remplissent les conditions énumérées par les articles 323-1 et suivants. Le texte évoque les outils *« conçus ou spécialement adaptés »* pour commettre des atteintes au STAD, un critère qui dépend directement de l'intention de l'auteur du logiciel. Malgré cette imprécision, il semble évident que le malware étudié par reverse engineering est un élément *« conçu ou spécialement adapté »* pour commettre des atteintes au STAD.

1.2.1.2 L'ingénierie inversée du malware doit être motivée par un motif légitime

L'article 6 de la Convention sur la cybercriminalité exclut la responsabilité pénale en cas de diffusion ou de mise à disposition d'un dispositif permettant une infraction informatique lorsque ces dernières « *n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique* ». Pour le professeur Agathe Lepage, le motif légitime doit également être entendu de façon à « *tenir compte des nécessités de la recherche ou de la sécurité informatique* »[42].

Mais l'article 323-3-1 n'évoque que le simple « motif légitime », sans en donner de définition claire. On peut donc encore légitimement penser que la finalité de sécurité informatique défensive guidant l'analyse de reverse engineering entre dans la définition du motif légitime évoqué dans l'article 323-3-1 du Code pénal. Les usages offensifs du reverse engineering semblent quant à eux exclus.

Sous-titre 2. Le test d'intrusion : quel cadre juridique ?

La simple analyse des vulnérabilités, même si elle est indispensable, demeure insuffisante[43]. Une démarche complémentaire de tests d'intrusion est parfois nécessaire. Point sur l'encadrement juridique du test d'intrusion.

D'un point de vue pratique, le test d'intrusion se déroule tout d'abord par une étude contextuelle du système : récolte de données publiques et scan protocolaire (TCP, UDP, ICMP), identification des systèmes d'exploitation et des services. Par la suite, l'auditeur entame le travail de recherche et d'identification de vulnérabilités. A l'issu du test d'intrusion, l'auditeur remet un rapport qui intègre

---

présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.
3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

[41] En plus d'une dizaine d'année, ce texte a été ratifié par 33 pays et signé par 14 autres[41]. Au total, ce sont plus de 120 pays qui collaborent de près ou de loin avec le Conseil de l'Europe pour lutter contre la cybercriminalité.

[42] Ibid.

[43] « *C'est pourquoi les tests d'intrusion, en particulier, sont devenu la pierre angulaire de la validation des vulnérabilités.*» rappelle Mark Hatton, Pdg de Core Security Technologies.

la liste des vulnérabilités, failles, risques et menaces découvertes. L'auditeur y délivre son expertise afin de déterminer l'impact de ces vulnérabilités sur le système d'information du client. Enfin, le testeur émet une série de mesures curatives : il peut s'agir de mises à jour logicielles, de la mise en place de nouvelle(s) configuration(s), de modification de l'architecture réseau, ou encore de redéfinition des politiques de sécurité. Ce rapport peut également aboutir à un plan de continuité d'activité (PCA) ou d'un plan de secours informatique.

1.3 La contractualisation du Pen Test

Le contrat de test d'intrusion permet généralement de **délimiter le champ d'intervention de l'auditeur**. Il définit notamment les méthodologies qui seront employées, les modalités d'exécution du test (*notamment Black box, White box ou encore directement depuis un compte utilisateur*), le périmètre de l'analyse, les moyens utilisés, la durée et/ou la périodicité du test, la mise en place d'une sauvegarde préalable, la coopération du SI, les règles de confidentialité, etc.

Le contrat comporte également les principes déontologiques qui guideront ce test d'intrusion. Mais surtout, ce contrat constitue pour l'auditeur une **habilitation** qui lui permettra d'opérer en toute légalité. Cependant, le système audité étant souvent dépendant de plusieurs prestataires (*hébergeurs, providers, etc.*), il est utile de prévoir contractuellement, à la charge de l'audité, l'obtention préalable d'**autorisations auprès de ses propres sous-traitants**. Le retrait de l'habilitation rend évidemment le maintien de l'auditeur dans le système d'information, illégal.

1.4 Intrusion réseau et notion de contournement de dispositif de sécurité

De nombreux pays comme **la Norvège, la Finlande, les Pays-Bas, la Suisse et le Luxembourg** exigent pour qu'il y ait intrusion dans un système d'information la présence ou la violation d'un dispositif de sécurité. En France, le juge considère que « *la protection d'un système de traitement automatisé de données par un dispositif de sécurité n'est pas une condition de l'incrimination*[44] » d'accès frauduleux dans un STAD[45]. Le juge français estime ainsi qu'il est nécessaire de rechercher l'intention de l'administrateur du système de restreindre ou non, l'accès au STAD. C'est en ce sens que la Cour d'appel de Paris, dans un arrêt du 30 octobre 2002, a décidé qu'il « *ne peut être reproché à un internaute d'accéder […] aux parties d'un site qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation, ces parties de site, qui ne font […] l'objet d'aucune protection de*

[44] TGI Paris, 18 septembre 2008, 31ème Ch. Correctionnelle. Jurisprudence constante, voir notamment, CA Paris 5 avril 1994 : « Il n'est pas nécessaire, pour que l'infraction existe, que l'accès soit limité par un dispositif de protection ».
[45] En revanche, il faut cependant souligner en ce qui concerne les opérateurs d'importance vitale[45] (OIV), que le Code la Défense oblige que les administrateurs de ces derniers établissent la liste les points d'importance vitale de son infrastructure en annexe de son plan de sécurité pour l'OIV.

la part de l'exploitant […], devant être réputées non-confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès. » Afin de savoir s'il y a eu accès frauduleux, il est dès lors nécessaire de rechercher l'intention de l'administrateur du STAD : existe-t-il une indication explicite ? L'administrateur a-t-il délivré une autorisation ?

L'affaire récente ayant opposé le blogueur Bluetouf à l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail est venue préciser ces éléments de jurisprudence. Par un jugement du 23 avril 2013, le tribunal correctionnel de Créteil a relaxé le blogueur, estimant que *« si le responsable d'un système d'information ne le sécurise pas contre les intrusions, le délit d'accès et de maintien frauduleux n'est pas constitué ».* Cette décision qui semble, de prime abord, contraire aux arrêts précédents ne fait que préciser leur portée. Le tribunal ayant conclu que *« même s'il n'est pas nécessaire pour que l'infraction existe que l'accès soit limité par un dispositif de protection, le maître du système, l'Anses, en raison de la défaillance technique, n'a pas manifesté clairement l'intention de restreindre l'accès aux données récupérées par [ndlr le prévenu] aux seules personnes autorisées ».*

1.5 Le *scan* de ports : une légalité à géométrie variable

Le *scan* ou *balayage de ports* est une technique consistant à rechercher les ports ouverts sur un système d'information, afin d'obtenir des informations sur son niveau de sécurité. Les « ports » sont des points d'entrée par lesquels une machine va pouvoir communiquer et échanger des informations avec d'autres ordinateurs ou services. Les balayages de ports sont dans leur grande majorité effectués sur le protocole TCP, mais certains logiciels, en général moins fiables, utilisent le protocole UDP ou ICMP.

La problématique juridique qui entoure le *scan* de port, est qu'il s'agit d'une **action susceptible de servir différentes finalités**. En effet, cette technique est couramment utilisée par les administrateurs systèmes et les ingénieurs logiciels pour contrôler la sécurité de leur réseau, mais elle peut aussi être utilisé par des pirates désirant cibler les failles d'un réseau informatique. Ainsi, d'un point de vue juridique, **cette pratique doit dès lors être observée en fonction des finalités poursuivies par son auteur**. Les juges ne sanctionnent d'ailleurs que très rarement cette pratique lorsqu'elle n'est pas un **acte préparatoire** à la commission d'une infraction.

En France, l'article **323-1 du Code Pénal**, ne semble pas applicable au scan de port, car cette technique n'implique aucun accès ou un maintien dans un STAD[46]. Cependant, le scan de port, en considération de sa nature, pourrait être assimilé à une tentative d'intrusion[47] dans la mesure où il peut s'apparenter à un acte préparatoire à une intrusion. Pour qu'il y ait tentative, il est toutefois

[46] STAD : Système de Traitement Automatisé de Données.
[47] Article 323-7 du Code Pénal français: « *La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.*»

nécessaire qu'il y ait commencement d'exécution, ce qui renvoie directement à la notion d'intention. Il s'agit dès lors d'une question de fait soumise au cas par cas à l'appréciation souveraine des juges du fond. Mais le scan de port peut être sanctionné sur le fondement de l'article **323-3-1** du même Code[48]. Cet article impose néanmoins d'une part que le logiciel ait été conçu spécialement pour la commission d'infractions et, d'autre part, que son utilisateur n'ait aucun motif légitime à utiliser ce type d'outil. Bien que cette différenciation puisse paraitre simple pour des logiciels répandus, elle sera beaucoup plus ténue lorsqu'il s'agira d'outils développés de façon plus artisanale.

Il est intéressant de préciser qu'une approche relativement similaire a été adoptée **en droit allemand**. La section **202c StGB *of the computer crime law*** dispose qu'il est prohibé, de « *posséder, vendre, distribuer, créer, utiliser des logiciels qui pourraient être utilisés comme outils de piratage* ». Et la simple possession d'outils n'a pour l'heure actuelle pas été sanctionnée. La jurisprudence[49] de la **Cour Constitutionnelle allemande** s'attache en effet principalement à l'intention de l'auteur. Le critère français de motif légitime de détention, c'est-à-dire la qualité de l'auteur, n'a pas été retenu en droit allemand.

En Angleterre, l'approche est analogue puisque le ***Police and Justice Act*** (2006) énonce que la fourniture ou l'offre de fourniture de moyens susceptibles d'être utilisés pour commettre, ou pour aider à la perpétration d'une infraction prévue au ***Computer Misuse Act*** (1990), est passible de 6 mois à 5 ans d'emprisonnement et d'une amende. Ici encore, le juge portera principalement son attention sur l'élément moral de l'infraction.

Dans les pays nordiques aussi, le critère porte principalement sur cet élément moral. Ainsi, dans une décision de la **Cour suprême finlandaise**[50], le juge a condamné l'auteur d'un scan de port, sur le fondement de la tentative d'intrusion informatique dans un système d'information, car ce dernier avait l'intention de s'introduire dans un réseau bancaire finlandais mais n'y était techniquement pas parvenu.

Aux États-Unis, il est intéressant de signaler que l'élément intentionnel est explicitement prévu par le ***Computer Fraud and Abuse Act*** (1986)[51], mais le juge combine également ceci à la notion d'accès autorisé et de dommage causé. Ainsi, dans une affaire célèbre de novembre 2011[52], le juge a estimé que le scan de port n'était pas un acte d'intrusion dans la mesure où il n'y avait eu aucun dommage, ni aucune altération de l'intégrité ou de la disponibilité du réseau.

---

[48] Article 232-3-1 du Code Pénal français : « *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.*»

[49] Déc. Cour constitutionnelle allemande, 18 mai 2009.

[50] Finnish Supreme Court, on April, 9, 2011; Esa Halmari Attorney (2003), Retrieved 2009-05-07.

[51] Notamment, 18 USC Sec. 1030(a)(5)(B): "*intentional accessing [of] a protected computer without authorization, [that] as a result of such conduct, recklessly causes damage*".

[52] Scott Alan Moulton vs. VC3, N° 1:00-CV-434-TWT.

En outre, il est possible de préciser qu'en ce qui concerne **Israël**, le juge se fonde sur la notion de tentative d'accès non autorisée sur du matériel informatique[53]. Il va même au-delà en retenant d'une part que l'intention de l'auteur n'était pas de pénétrer le système d'information, en l'espèce du Mossad, mais surtout qu'**il a agi dans l'intérêt général en démontrant l'existence d'une vulnérabilité**.

[53] Sur le fondement de la stion 4 de la Computers Law, (1995) et de la section 34 of the Penal Law, 5377 (1977).