Cyber sécurité et attaques informatiques : les leçons à tirer de Wanna Cry et Not Petya

Ève Tourny

Cyber sécurité et attaques informatiques : les leçons à tirer de Wanna Cry et Not Petya :

Eve Tourny

Juriste cyber au sein du Ministère des armées[1]

Wanna Crypt et Not Petya : ces deux noms ont semé la panique dans le monde numérique. Les conséquences de ces ransomwares auraient pu néanmoins être évitées si les utilisateurs avaient mis en œuvre des mesures de bon sens. L'importance de ces mesures est d'autant plus grande que la responsabilité pénale des victimes peut être mise en cause et cela plus aisément que celle des auteurs.

Wanna crypt and Not Petya has caused great fear all around the digital world. Nonetheless, the negative ransomwares' consequences could have been avoided by simple measures. These measures are so crucial that it's easier to incur victim criminal liability than to sue or even identify ransomware author.

ransomware, règlement général sur la protection des données à caractère personnel, Commission Nationale Informatique et Liberté, directive NIS, convention cybercrime, souveraineté numérique.

ransomware, General Data Protection Regulation, French Data Protection Authority, Network and Information Security European Directived, convention on cybercrime, digital sovereignty.

I.Introduction

« Oops, your files have been encrypted ». Voilà le message que certains utilisateurs ont eu la mauvaise surprise de découvrir début mai 2017 en allumant leur ordinateur, victimes d'un ransomware.

Le ransomware, ou rançongiciel, est un logiciel indésirable qui prend en otage les données et exige une rançon en échange de la clef de déchiffrement qui permettra, aux dires des auteurs du ransomware[2], de récupérer les données. Dans la très grande majorité des hypothèses, il s'agit d'une rançon pécuniaire, le plus souvent payable en bitcoin[3]. Mais, certains ransomwares font preuve d'originalité : ainsi du ransomware Popcorn Time qui propose à l'utilisateur victime une alternative au paiement en bitcoin ; aider le logiciel à s'installer sur au moins deux autres ordinateurs. De même au début des années 2010, des utilisateurs ont reçu un message leur indiquant que des images pédopornographiques avaient été dissimulées sur leur ordinateur et que, sauf paiement de leur part, ils feraient l'objet d'une dénonciation auprès des services de police[4].

La communauté informatique s'accorde à dire que le premier ransomware est apparu à la fin des années 80. Néanmoins, une augmentation significative de ce phénomène est à

[1] Les opinions exprimées dans cet article n'engagent que leur auteur et ne reflètent pas la position du Ministère des armées.

[2] Dans le cas du ransomware Not Petya, les spécialistes ont prévenu que la récupération des données était impossible. Cf. not J. COX, "Hacker behind massive ransomware outbreak can't get emails from victims who paid", 27 juin 2017, disponible sur https://motherboard.vice.com/en_us/article/new8xw/hacker-behind-massive-ransomware-outbreak-cant-get-emails-from-victims-who-paid

[3] Le bitcoin est une monnaie électronique qui n'est gérée par aucune banque. Cf. https://bitcoin.fr/

[4] Cf. R. MC MILLAN « Alleged Ransomware Gang Investigated by Moscow Police », 31 août 2010, disponible sur http://www.pcworld.com/article/204577/article.html

souligner depuis 2016. L'éditeur de logiciel Symantec[5] dans son dernier rapport annuel, mettait l'accent sur la menace grandissante véhiculée par le ransomware[6]. Force est de constater que le premier semestre 2017 a montré la véracité de ses prédictions.

Début mai, le ransomware Wanna Crypt[7] infecte plusieurs centaines de milliers d'ordinateurs dans plus de 150 pays[8]. Le mois suivant c'est le ransomware Not Petya qui sévissait. Ces deux attaques permettent de présenter un certain nombre de considérations techniques - comment ont été propagés ces ransomwares, quelles ont été les victimes et quels sont les moyens de s'en protéger ? (II) – et offrent la possibilité d'étudier leurs conséquences sur le plan juridique (III)

II.Wanna Crypt et Not Petya , une cybercriminalité maîtrisable bien que mondialisée

De par leur mode de propagation les deux ransomwares ont fait de nombreuses victimes à travers le monde (I.1.). Pour autant, les bonnes pratiques à mettre en place pour lutter contre ce phénomène ou en amoindrir les conséquences ne nécessitent pas une haute expertise technique et n'ont pas un fort impact financier (I.2.).

II.1.Wanna Crypt et Not Petya, ransomwares aux dimensions internationales.

Wanna Crypt se propage par le biais de l'exploit informatique[9] Eternal Blue créé par la NSA[10] et révélé début avril par un groupe de hackers dénommé the Shadow Brokers. Not Petya tient son nom d'un précédent ransomware, Petya, qui a sévit en mars 2016. En effet, au début de la propagation de Not Petya, certains spécialistes ont pensé à un retour de ce ransomware sous une nouvelle version. La société de sécurité informatique russe Kaspersky a rapidement infirmé ces affirmations en faisant valoir que ce ransomware présentait de trop grandes différences avec Petya pour pouvoir être considéré comme un dérivé. C'est la raison pour laquelle il a été dénommé Not Petya[11]. Not Petya exploite le même outil de propagation que Wanna Crypt, des failles de sécurité, mais ce ne sont pas les mêmes. C'est la raison pour laquelle certains ordinateurs, qui n'avaient pas été infectés par Wanna Crypt, l'ont été par Not Petya.

Les premiers rapports montrent que les principales victimes ont été des organisations, publiques et privées, et non des particuliers. La raison qui peut être évoquée est la recherche de la rentabilité de l'opération ; une fois installé sur une machine d'une organisation, le ransomware peut se propager à l'ensemble des machines connectées au réseau et réclamer une rançon pour chaque ordinateur infecté. C'est ainsi que Wanna Crypt a touché l'opérateur de téléphonie espagnol Telefonica, la compagnie américaine de transport Fedex, des universités

[5] Symantec édite notamment le logiciel antivirus Norton.

[6] Cf. SYMANTEC, *Internet Security Threat Report n°22*, avril 2017, disponible sur https://www.symantec.com/fr/fr/security-center/threat-report

[7] Dénommé rapidement Wanna Cry pour le jeu de mot.

[8] Ce ne sont que des estimations. Il est en effet plus que probable que certaines victimes aient préféré rester silencieuses pour éviter les conséquences d'une publicité négative.

[9] Un exploit informatique est un appareil ou une méthode utilisé pour profiter d'une vulnérabilité existante au sein de n'importe quel matériel ou logiciel.

[10] Cf. « NSA Malware released by Shadow Brockers Hacker Group », 10 avril 2017, disponible sur http://www.bbc.com/news/technology-39553241

[11] Cf. « New Petya/ NotPetya/ExPetr ransomware outbreak », 28 juin 2017, disponible sur https://www.kaspersky.com/blog/new-ransomware-epidemics/17314/

chinoises ou encore des hôpitaux britanniques. La France n'a pas été épargnée puisque Renault figure au rang des victimes[12].

Not Petya quant à lui a visé les grandes banques ukrainiennes, l'entreprise Mars, le pétrolier russe Rosneft, l'entreprise française Saint-Gobain ou encore le laboratoire américain Merck[13].

II.2. Des moyens de protection faciles à mettre en œuvre

Les mesures à adopter pour éviter d'être victime d'un ransomware ou en amoindrir les conséquences ne nécessitent pas d'être un spécialiste de la sécurité informatique (II.2.1.). Elles doivent néanmoins s'inscrire dans un document plus large qui est le Plan de Continuité d'Activité /PRA (II.2.2.). De plus, en cas d'interrogations ou de difficultés, des structures ont été créées dans le cadre français pour apporter une aide et des solutions, contribuant à réaliser un dispositif performant en matière de sécurité des systèmes d'information (II.2.3.)

II.2.1. Des moyens de protection de faible technicité.

Quelle que soit la virulence des cyberattaques, des mesures simples et de bon sens constituent la première protection. Wanna Crypt et Not Petya utilisant tous deux des failles de sécurité, la meilleure des protections passe par une mise à jour régulière des logiciels et du système comme le rappelle l'Agence Nationale de Sécurité des Systèmes d'Information[14]. Il est également impératif de procéder à une sauvegarde régulière des données. En cas de chiffrement des données stockées sur un ordinateur, cela permet de ne pas subir de conséquences puisqu'il y a alors la possibilité d'utiliser les données sauvegardées. Néanmoins, une sauvegarde seule n'est pas suffisante : il importe de procéder à des tests de manière à vérifier que le processus s'est correctement effectué[15].

D'autres bonnes attitudes sont également à développer afin de se prémunir d'un ransomware dont le vecteur de propagation serait une pièce jointe d'un mail piégé[16] ou encore un lien internet infecté présent dans le corps d'un mail. Pour éviter de subir les conséquences liées à ces modes de propagation, le seul bon sens suffit ; ne pas ouvrir de messages provenant d'expéditeurs inconnus et faire preuve de vigilance envers les liens contenus dans les mails[17]. Une sensibilisation du personnel des administrations et des entreprises n'est toutefois pas superflue afin qu'il acquière les bons réflexes[18]. Wanna Crypt et Not Petya ont démontré que

---

[12] Cf. X. RAUFER, « Wanna Cry le cyber désastre dont la France tente de se protéger avec une nouvelle ligne Maginot », 19 mai 2017, disponible sur http://www.atlantico.fr/decryptage/wanna-cry-cyber-desastre-france-tente-se-proteger-avec-nouvelle-ligne-maginot-xavier-raufer-3048705.html

[13] Cf. « Not Petya une lueur d'espoir dans la quête des données perdues », 11 juillet 2017, disponible sur http://www.itespresso.fr/notpetya-lueur-espoir-donnees-perdues-165172.html?inf_by=584a70772ad0a1da2c1885aa

[14] Site officiel de l'ANSSI http://sssi.gouv.fr

[15] Cf. ANSSI, alerte aux rançongiciels, vos données en otage contre de l'argent, disponible sur https://www.ssi.gouv.fr/uploads/2016/06/20160819_flyers_eben_a4_v10.pdf

[16] Ainsi du ransomware Locky. Cf. not. L. ADAM « Locky : une nouvelle vague d'e-mails malveillants détectée », *ZDNet*, 25 avril 2017, disponible sur http://www.zdnet.fr/actualites/locky-une-nouvelle-vague-d-e-mails-malveillants-detectee-39851658.htm

[17] Pour une démonstration cf. CIGREF, Campagne hack Academy, Willy disponible sur https://www.hack-academy.fr/candidats/willy

[18] Pour des exemples de sensibilisation cf. vidéos de sensibilisation du CIGREF, https://www.hack-academy.fr/

ces principes de base n'étaient pas suivis. Ainsi, selon un sondage réalisé en France en 2016, seulement 27% des entreprises interrogées avaient procédé à une sensibilisation de l'ensemble de leur personnel sur ces questions[19].

Wanna Crypt et Not Petya doivent également amener les dirigeants à examiner la protection des données de leurs structures sous un angle plus global et s'assurer notamment qu'elles disposent d'un Plan de Continuité d'Activité ou Plan de Reprise d'Activité (PCA/PRA), atout majeur dans la protection des données.

II.2.2. L'adoption d'un plan de continuité d'activité, renforcement de la lutte contre le ransomware.

Le plan de continuité d'activité regroupe les actions techniques et organisationnelles à mettre en place pour assurer la mission en mode dégradé et le retour à un mode nominal ou normal . Le plan de reprise d'activités ne vise que le retour au mode nominal.

Un PCA vise l'ensemble des actifs d'une entreprise, qu'ils soient financiers, humains ou matériels ainsi qu'un volet informatique. Dans ce dernier domaine, l'établissement d'un PCA suppose une identification des risques et de leurs conséquences et une identification des données les plus stratégiques pour la structure. Il faut ensuite, pour chaque risque, envisager des procédures permettant de protéger ces données, soit en faisant disparaître le risque, soit en en diminuant les impacts, soit en le transférant à un tiers, soit en l'acceptant[20]. Cette démarche doit associer tous les décideurs de la structure et nécessite une connaissance fine de l'organisation, de son cœur de métier et de son mode de fonctionnement. En effet, la mise en place des procédures a un coût et il est rarement possible, d'un point de vue financier, d'accorder la même protection à l'ensemble des données ou des services d'une entreprise[21].

Outre la norme ISO 22301 qui permet d'établir un PCA, les entreprises peuvent également s'appuyer sur des guides établis notamment par le Secrétariat Général de la Défense et de la Sécurité Nationale[22], et les recommandations de l'ANSSI, deux structures de haut niveau dans le dispositif de sécurité des systèmes d'information en France.

---

[19] Cf. https://fr.statista.com/statistiques/586048/sensibilisation-du-personnel-au-systeme-information-entreprises-francaises/

[20] La norme ISO 22301 permet de mettre en place et de contrôler un système de management de la continuité d'activité.

[21] Il est ainsi possible de prévoir que les données seront sauvegardées en temps réel. Mais le coût est important. Il est alors nécessaire de hiérarchiser les données et de ne prévoir une sauvegarde en temps réel que pour les données les plus stratégiques. Les entreprises qui passent les ordres boursiers ainsi que la française des jeux, possèdent une réplication en temps réel des données ainsi que des sites miroirs qui permettent aux employés de continuer à travailler sur un lieu géographiquement différent sans aucune coupure. Ces moyens mis en place et le coût engendré se justifie au regard de la criticité des activités.

[22] Guide disponible à https://www.economie.gouv.fr/files/hfds-guide-pca-plan-continuite-activite_sgdsn.pdf

II.2.3. L'intervention du dispositif national de sécurité des systèmes d'information.

L'ANSSI a été créée par décret le 7 juillet 2009[23]. Rattachée au SGDSN, elle est l'autorité nationale en matière de sécurité des systèmes d'information[24]. Elle dispose d'une mission de sensibilisation, de contrôle des systèmes d'information étatiques ainsi que d'élaboration de la politique de sécurité des systèmes d'information au niveau national. La France dispose également de Computer Emergency Response Teams, structures d'alerte et d'assistance sur l'internet qui sont chargées d'une mission de veille et de réponse aux attaques informatiques[25].

D'autres structures participent à l'amélioration de la sécurité des systèmes d'information notamment en mettant à disposition des sensibilisations. C'est notamment le cas du Club Français de la Sécurité de l'Information Français[26] ou encore du CIGREF, réseau de grandes entreprises dont la mission est de « développer la capacité des grandes entreprises à intégrer et maîtriser le numérique. Il compte aujourd'hui 140 grandes entreprises et organismes français[27].

Le dispositif français de sécurité des systèmes d'information est donc bien établi et l'ANSSI notamment met à disposition des plaquettes de vulgarisation et d'information aux dangers de ce type. Pour autant, les entreprises sont encore trop peu conscientes de la menace et de ses conséquences multiples.

III. Le ransomware, manifestation de cybercriminalité aux multiples conséquences juridiques.

L'impact d'un ransomware peut se manifester sur plusieurs plans. Ainsi, dans l'hypothèse d'une entreprise telle que Renault, le ransomware a eu à la fois un impact financier, l'arrêt des chaînes de production entraînant des pertes d'exploitation mais également un impact sur la réputation. L'annonce dans les médias que Renault est victime d'un ransomware est une publicité négative pour l'entreprise. Le ransomware produit également des effets dans le domaine juridique, celles-ci concernant aussi bien la victime du ransomware (III.1.) que son auteur (III.2.).

III.1. La poursuite de la victime sur le fondement du droit national.

Paradoxalement, c'est la victime du ransomware qui peut être le plus aisément mise en cause. Deux hypothèses doivent être envisagées ; celle dans laquelle le ransomware a visé des données à caractère personnel et celle dans laquelle un système d'information d'importance vitale a été touché.

Lorsque des données à caractère personnel sont en cause, le régime juridique est très protecteur. Dans l'hypothèse où le ransomware aurait visé ce type de données, le responsable

[23] Décret 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « agence nationale de la sécurité des systèmes d'information ».

[24] Art. 3 du décret 2009-834.

[25] Pour la liste des CERT cf. https://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/les-cert-francais/ et le site officiel du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques http://www.cert.ssi.gouv.fr/

[26] Site officiel du CLUSIR : https://clusir.fr/

[27] Site officiel du CIGREF : www.cigref.fr/

du traitement peut voir sa responsabilité engagée sur le fondement de la loi du 6 janvier 1978[28] au motif qu'il n'a pas protégé les données[29]. Le responsable du traitement encourt une sanction pécuniaire qui peut atteindre trois millions d'euros[30]. Il est à noter que le régime juridique des données à caractère personnel, déjà très protecteur, va se durcir avec l'entrée en vigueur en mai 2018 du règlement général sur la protection des données à caractère personnel[31] ou RGDPD. Le RGPDP prévoit notamment un système de sanction pécuniaire qui peut aller jusqu'à vingt millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent. Le texte précise que le montant le plus élevé sera retenu[32].

Les conséquences juridiques seront différentes dans l'hypothèse où un système d'information d'importance vitale (SIIV) aura été touché par le ransomware. Selon l'ANSSI, un SIIV est un « système pour lequel l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ». Suite au Livre Blanc sur la défense et la sécurité nationale de 2013[33], l'article 22 de la loi de programmation militaire (LPM)[34] a inséré dans le code de la défense des articles relatifs à la sécurité des systèmes d'information[35]. L'article L. 1332-6-1 prévoit notamment que le premier ministre fixe les règles de sécurité nécessaires à la protection des systèmes d'information pour les opérateurs d'importance vitale (OIV).

Un OIV exerce des activités mentionnées à l'article R. 1332-2 du code de la défense et comprises dans un secteur d'activité d'importance vitale. De plus, il gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement, d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population. Un décret mentionne l'intégralité des 200 OIV en France[36]. Suite à la LPM, des arrêtés sectoriels ont été pris. Ils font peser sur les OIV des obligations afin de s'assurer de la sécurité des systèmes d'information d'importance vitale. Les OIV sont tenus de déclarer à l'ANSSI, leurs SIIV. Ils ont également l'obligation de déclarer à l'Agence tout incident de sécurité et ce sans délai. Les arrêtés prévoient aussi que chaque OIV se dote d'une politique de sécurité des systèmes d'information (PSSI). La PSSI permet d'exposer les orientations stratégiques et peut aussi être utilisée comme instrument de sensibilisation et de communication[37]. Ils doivent enfin prévoir des mesures pour garantir la

[28] Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Disponible sur https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460

[29] Article 34 de la loi du 6 janvier 1978 « le responsable du traitement est tenu de prendre toutes précautions utiles au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et notamment, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès ».

[30] Article 47 de la loi du 6 janvier 1978.

[31] Règlement (UE) 2016/679 du Parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE. Texte disponible sur http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR

[32] Cf. Article 83 « conditions générales pour imposer des amendes administratives » du RGDPD.

[33] Document disponible sur http://www.livreblancdefensetsecurite.gouv.fr

[34] Loi 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 portant diverses dispositions concernant la défense et la sécurité nationale. Texte disponible sur https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&categorieLien=id

[35] Articles L. 1332-6-1 à L. 1332-6-6 du code de la défense.

[36] Pour des raisons de sécurité nationale ce décret est classifié.

[37] A titre d'exemple, l'Etat s'est doté d'une PSSI-A de laquelle a été déclinée une PSSI pour chaque

traçabilité des accès aux SIIV, leur maintien en condition de sécurité ou encore prévoir l'homologation de sécurité de ces systèmes[38].

Sur ces aspects, l'Union européenne a adopté le 6 juillet 2016 une directive sur la sécurité des réseaux et des systèmes d'information ou directive NIS[39]. Cette directive vise les opérateurs de services essentiels ou OSE. Un OSE est une entité qui fournit un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques. La fourniture de ce service est tributaire des réseaux et des systèmes d'information et un incident aurait un effet disruptif important sur la fourniture dudit service[40]. Ce texte met à la charge des OSE des exigences de sécurité et de notification d'incidents[41]. Il est à remarquer que les obligations créées par la directive NIS sont semblables à celles présentes dans la législation française. La principale différence réside dans le champ d'application de la directive. En effet, alors que le nombre d'OIV s'élève à 200, ce nombre va être décuplé avec la directive NIS et les OSE[42].

Ces conséquences juridiques pour les responsables des traitements de données ou les responsables de SIIV sont d'autant plus importantes que les auteurs des ransomwares, à l'instar d'autres formes de cybercriminalité, ne sont que rarement poursuivis.

III.2. L'impossible poursuite des auteurs de ransomwares.

Ce n'est pas l'insuffisance des dispositions juridiques sur le fondement desquelles peuvent être exercées les poursuites mais les difficultés de leur identification qui font que les auteurs de ransomwares sont rarement poursuivis. L'arsenal répressif sur le plan national s'avère désormais mature. Il permet de lutter contre la cybercriminalité ce qui recouvre les infractions dans lesquelles le réseau est le vecteur et celles dans lesquelles le réseau est la cible. La première catégorie ne soulève pas de difficultés du point de vue des poursuites : les dispositions incriminant les infractions existent et le fait que l'informatique soit un vecteur n'est pas un élément constitutif. Ainsi dans le cas d'une escroquerie, l'article sur le fondement duquel vont s'exercer les poursuites vise tant l'escroquerie commise dans le monde physique que celle commise par le biais des réseaux[43]. Dans le cas de la pédopornographie, l'utilisation

---

ministère. La PSSI-E est disponible sur https://www.ssi.gouv.fr/uploads/IMG/pdf/pssie_anssi.pdf

[38] Pour un exemple d'arrêt sectoriel, cf. arrêté du 28 novembre 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activité d'importance vitale « finances » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense. Texte disponible sur https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=A590DC7FE86CF4C8E1964312C24F08C0.tpdila07v_1?cidTexte=JORFTEXT000033518925&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000033518910

[39] Directive 2016/1148 du Parlement européen et du conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. Texte disponible sur http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=FR

[40] Cf. Article 5 « identification des opérateurs de services essentiels » de la directive NIS.

[41] Cf. Article 14 « exigences de sécurité et notifications d'incidents » de la directive NIS.

[42] A titre d'exemple, à l'heure actuelle seuls certains aéroports français sont considérés comme étant des OIV. Sous l'empire de la directive NIS, l'ensemble des aéroports sera considéré comme OSE.

[43] Article 313-1 du code pénal : *« l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.*

L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende ».

d'un réseau sera une circonstance aggravante[44]. S'agissant des infractions dans lesquelles le réseau est la cible, la France s'est dotée assez tôt d'un arsenal répressif qui repose sur la loi « Godfrain » de 1988. Celle-ci insère dans le Code pénal des articles permettant de réprimer les atteintes aux systèmes de traitement automatisé de données[45]. L'auteur d'un ransomware peut ainsi être poursuivi pour avoir accédé, s'être maintenu frauduleusement[46] et avoir entravé le fonctionnement de ce système[47]. Le cas échéant, pourra également être poursuivie la personne qui a fourni les moyens pour commettre cette infraction[48].

Toute la difficulté réside alors dans l'identification de l'auteur du ransomware. Les techniques informatiques permettent en effet de dissimuler son identité et ses actions dans le cyberespace. Dès lors, il est extrêmement complexe de prouver l'identité de l'auteur. Ne pèsent le plus souvent que de fortes présomptions qui sont impossibles à corroborer. Ainsi, dans l'hypothèse du ransomware Not Petya, les premières victimes ayant été des banques ukrainiennes, il a été suggéré que l'attaque avait été lancée depuis la Russie. Néanmoins, la propagation aux infrastructures russes est venue remettre en doute cette affirmation.

Pour les mêmes raisons, la rumeur selon laquelle Wanna Crypt serait d'origine russe est difficile à croire puisque le ransomware s'est attaqué également à des systèmes russes. Dans ce dernier cas, les soupçons se portent désormais sur la Corée du Nord. La seule exception, car un des auteurs l'a revendiqué, concerne le virus Stuxnet qui s'est attaqué aux centrifugeuses de la centrale nucléaire iranienne de Natanz en 2009[49]. Lors de sa réélection, le président américain B. Obama a reconnu que les Etats-Unis avaient été partie prenante dans l'élaboration de ce virus. Sans qu'il y ait de preuve formelle, il semblerait que Stuxnet résulte de la coopération entre les Etats-Unis et Israël.[50]. Ainsi, seul l'aveu pourrait permettre d'identifier l'auteur d'un ransomware.

---

[44] Article 227-13 du code pénal « *le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Lorsque l'image ou la représentation concerne un mineur de quinze ans, ces faits sont punis même s'ils n'ont pas été commis en vue de la diffusion de cette image ou représentation.*

Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines

Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques ».

[45] Articles 323-1 à 323-8 du code pénal.

[46] Article 323-1 du code pénal : « *le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000€ d'amende* ».

[47] Article 323.2 du code pénal : *« le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000€ d'amende ».*

[48] *Article 323-3-1 du code pénal « le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou tout données conçu ou spécialement adapté pour commettre une ou plusieurs 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] Pour une présentation complète de Stuxnet cf. not. XMCO, « Stuxnet : analyse, mythes et réalités », *L'actu Sécu 27*, Février 2011, disponible sur https://www.xmco.fr/actu-secu/XMCO-ActuSecu-27-STUXNET.pdf

[50] S. LEBLAL, « Barack Obama a ordonné les attaques Stuxnet contre l'Iran », *Le monde informatique*, 1er juin 2012, disponible sur http://www.lemondeinformatique.fr/actualites/lire-barack-obama-a-ordonne-les-attaques-stuxnet-contre-l-iran-49147.html

Dans la quasi-totalité des hypothèses l'auteur n'est donc pas poursuivi car son identification formelle ne peut avoir lieu. L'imputabilité d'une action n'est pas pour autant synonyme de poursuites. Si l'auteur identifié est un individu isolé, sa répression est possible. Mais il est des hypothèses qui soulèvent d'importants questionnements juridiques quant aux poursuites : ainsi l'action d'un groupe travaillant au profit d'un Etat, celle d'un groupe travaillant au profit d'un Etat situé sur le territoire d'un Etat tiers, celle d'un groupe travaillant au profit d'un Etat mais qui n'est pas financé par ce dernier[51]. Dans ces hypothèses qui poursuivre ? L'individu ? L'Etat, en mettant en cause sa responsabilité internationale pour fait illicite ? Dans tous les cas, la mise en œuvre des poursuites se heurtera à la difficulté à recueillir des preuves.

Dans l'hypothèse, juridiquement la moins complexe, d'un individu isolé sans lien avec une puissance étatique, il faut alors faire appel aux mécanismes de coopération internationale. La Convention de lutte contre la cybercriminalité signée à Budapest le 23 novembre 2001[52] prévoit ainsi des mécanismes adaptés à l'extrême volatilité des données informatiques[53]. Néanmoins, les enquêtes sont souvent longues. Ainsi, la plateforme criminelle « avalanche » découverte en 2012 a été démantelée fin 2016[54]. De plus, le dispositif mis en œuvre par la Convention de Budapest est jugé inefficient par les professionnels[55].

IV. Conclusion

L'inefficacité des mécanismes juridiques a notamment pour origine une absence de volonté de coopération de la part de certains Etats qui utilisent le cyberespace à des fins politiques et stratégiques[56] et qui considèrent que le cyberespace relève strictement des questions de souveraineté nationale. L'observation de la carte des Etats victimes de Wanna Crypt permet de constater que l'Asie n'a pas, ou très peu, été touchée. Si cela peut être une indication quant à l'origine du ransomware, il s'agit aussi d'une manifestation d'un phénomène qui tend à prendre de plus en plus d'ampleur : les Etats réaffirment leur souveraineté sur le cyberespace et cherchent à sécuriser ce domaine en évoquant la souveraineté numérique.

La stratégie de coopération internationale dans le cyberespace publiée par la Chine au début du mois de mars 2017 en est une illustration[57]. Dès le premier chapitre il est rappelé que le cyberespace constitue certes « *une nouvelle passerelle d'échanges et de coopération* » mais aussi « *un nouveau domaine où s'exerce la souveraineté nationale* ».

---

[51] Ainsi, les pirates russes œuvrent souvent pour leur « mère Patrie » alors qu'ils résident à l'étranger et certains le font par loyauté ou patriotisme sans compensation financière.

[52] Document disponible sur http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_fr.pdf

[53] Cf. Articles 16 à 21 de la Convention.

[54] Cf. S. DUMOULIN, « Une opération de police internationale fait tomber un large réseau de cybercriminalité », *les Echos*, 2 décembre 2016, disponible sur https://www.lesechos.fr/02/12/2016/lesechos.fr/0211557586627_une-operation-de-police-internationale-fait-tomber-un-large-reseau-de-cybercriminalite.htm

[55] C'est la position adoptée par A. SEGER, secrétaire exécutif du comité de la convention sur la cybercriminalité dans le cadre d'une conférence délivrée à Nouakchott les 9 et 10 mars 2015.

[56] Cf. A. DESFORGES, *La coopération internationale et bilatérale en matière de cybersécurité : enjeux et rivalités*, IRSEM, 2013, 18p.

[57] Cf. stratégie de la coopération internationale dans le cyberespace disponible sur http://www.fmprc.gov.cn/fra/wjdt/wjzc/ty/t1442395.shtml

Tout au long de ce document, il est rappelé la nécessité de la coopération et de la collaboration mais la notion de souveraineté est omniprésente[58]. La position de la Chine quant au concept de souveraineté numérique ne souffre d'aucune ambiguïté à la lecture du passage suivant : « *le principe de l'égalité souveraine est une règle fondamentale régissant les relations internationales contemporaines et valable dans tous les domaines des échanges interétatiques. Ce principe et son esprit doivent aussi s'appliquer au cyberespace. Les gouvernements nationaux ont le droit d'administrer en vertu de la loi le cyberespace, d'exercer, sur le territoire national, la juridiction sur les infrastructures, les ressources et les activités informatiques et de communication, de protéger les systèmes et ressources nationaux d'information contre toute menace, perturbation, attaque ou sabotage et de garantir les droits et intérêts légitimes de leurs citoyens dans le cyberespace* ». Par cette déclaration, la Chine légitime les textes de lois pris pour exercer un contrôle accru sur le cyberespace et il peut être déduit que ce phénomène va perdurer. Les Etats qui ne le font pas déjà ne peuvent qu'être enclins à faire de même et à affirmer également leur souveraineté numérique.

[58] Cf. Not. Chapitre II « *la Chine préconise le concept de développement équitable, ouvert, global et innovant, le concept global de sécurité commune, intégrée, coopérative et durable et les principes fondamentaux de la paix, de la souveraineté, de la gouvernance commune et des bénéfices pour tous pour tous les échanges et coopérations internationaux dans le cyberespace* ».