Du 30 septembre au 3 octobre ont lieu les Assises de la sécurité au Grimaldi Forum. Parmi les experts présents : Nicolas Arpagian. Le rédacteur en chef de la revue *Prospective Stratégique* [1] et directeur scientifique à l'Institut national des hautes études de la sécurité et de la justice (INHESJ), explique à *Monaco Hebdo* les risques de cyberattaques qui pèsent sur la Principauté. Cet expert évoque aussi le piratage du site adultérin Ashley Madison et les risques liés au cyberterrorisme.

PROPOS RECUEILLIS PAR SABRINA BONARRIGO

CYBERATTAQUE « MONACO EST ÉVIDEMMENT UNE CIBLE POTENTIELLE »

MI-AOÛT, LE SITE INTERNET DE RENCONTRES ADULTÈRES ASHLEY MADISON A ÉTÉ PIRATÉ ET LES DONNÉES PRIVÉES DE 32 MILLIONS DE MEMBRES ONT ÉTÉ MISES EN LIGNE : ÇA VOUS A SURPRIS ?
Non. Car les pirates cherchent toujours à voler ce qui a de la valeur. Dans l'affaire Ashley Madison, il y avait des noms, des orientations sexuelles, des éventuelles infidélités — ce qui peut permettre des opérations de chantage — et des coordonnées bancaires. Ces quatre éléments font qu'évidemment, c'était une cible prévisible. Ce qui est intéressant dans cette attaque, c'est de s'apercevoir que la promesse commerciale était mensongère.

C'EST-À-DIRE ?
Je ne suis pas un grand sociologue, mais ce site garantissait qu'il y avait plus de femmes que d'hommes à la recherche d'activités adultérines… C'est peut-être un fantasme d'homme, mais statistiquement on peut en douter. On ne fait pas un business model planétaire en affirmant que l'on dispose d'un fichier d'1 million de femmes adeptes de relations adultérines ! Cette affaire a donc permis de révéler l'escroquerie de l'argumentaire. En réalité, le site Ashley Madison est le plus gros site gay de la planète, avec grosso modo 9 hommes inscrits pour une femme ! C'est d'ailleurs à se demander combien de personnes ont réussi à concrétiser une relation. Il semblerait aussi qu'il y ait un volet d'activités de prostitution, manifestement à l'initiative des dirigeants du site.

LES PIRATES INFORMATIQUES SONT DE PLUS EN PLUS DOUÉS ?
Grâce à leur imagination, leur créativité et leur maîtrise technique, les pirates informatiques sont capables de contourner bien des systèmes de sécurité établis. Des activistes parviennent à harceler, et donc à mettre en difficulté, des adversaires disposant de moyens substantiels : entreprises, administrations ou même forces armées. De plus, les technologies de l'information et de la communication sont désormais partout… Aussi bien dans les structures administratives, économiques, commerciales, financières, industrielles que médicales ou militaires. Il faut ajouter aussi nos usages personnels de plus en plus numérisés : blogs, messageries instantanées, réseaux sociaux, télédéclarations fiscales…

LE PIRATAGE EST À LA PORTÉE DE TOUS ?
Amusez-vous à écrire sur un moteur de recherche : « Comment »… puis, taper les trois lettres suivantes : « p », « i » et « r »… Vous verrez que le premier lien que l'on vous propose est : « Comment pirater un compte Facebook. » Ce sont des tutoriels simplifiés qui vont vous permettre, sans avoir de grandes connaissances, de pirater votre voisin de bureau ou votre ex-petit ami…

C'EST AUSSI SIMPLE QUE ÇA ?
Les conseils sont livrés clés en main, étape par étape. Sur internet, on trouve aussi des pirates qui créent des sites pour proposer leur savoir-faire. Ce sont des offres présentées comme de banales prestations de service. Avec même des rabais pour ceux qui commandent plusieurs prestations…

ON A L'IMPRESSION QUE LES CYBERATTAQUES RESTENT DANS UNE TOTALE IMPUNITÉ ?
La lutte contre la cybercriminalité pâtit encore trop souvent de la lenteur des procédures de la coopération internationale. Le temps judiciaire est loin de correspondre au temps technologique… Il est donc certain qu'il y a une impunité relative.

CEUX QUI ONT PIRATÉ ASHLEY MADISON OU TV5 MONDE RISQUENT DE SE RETROUVER UN JOUR EN PRISON ?
Ce n'est pas le premier péril qui les guette… En droit pénal, il y a une notion qui s'appelle « l'imputabilité ». C'est-à-dire le fait de pouvoir attribuer la maternité d'une action. Or, on peut tout à fait commettre un acte illicite sur internet ou faire une campagne de dénigrement, en usurpant son identité, ou en affirmant que son ordinateur a été piraté… Le relatif sentiment d'impunité est donc un réel encouragement pour de futurs cyberdélinquants.

LES PERSONNES QUI ONT DES INTENTIONS CRIMINELLES ONT DONC INTÉRÊT À LES CONCRÉTISER EN RESTANT TRANQUILLEMENT DERRIÈRE LEUR ORDINATEUR…
Absolument. Ce n'est d'ailleurs pas un hasard si l'on voit que les braquages de banques chutent. Car braquer une banque demande un engagement physique. Il y a aussi l'aléa relatif à la somme plus ou moins grande que vous allez trouver dans la caisse. Vous pouvez avoir aussi des billets maculés avec des systèmes de sécurité, ou risquer de blesser voire de tuer quelqu'un… Autant commettre son acte tranquillement chez soi, derrière son ordinateur. Ce sont des virements numérisés. Et, encore une fois, il y a une relative impunité.

SUR INTERNET ON PEUT EN PLUS TOUCHER DES CIBLES TRÈS LARGES ?
Absolument. C'est ce que l'on appelle l'économie des moyens. Aujourd'hui, on peut envoyer un spam à 500 000 personnes en écrivant : *« Bonjour, c'est la Société des Bains de Mer (SBM), vous avez gagné au loto du casino de Monaco. Merci de cliquer ici pour donner vos coordonnées bancaires… »* Si sur 500 000 personnes, il y a 3 000 destinataires qui répondent… c'est jackpot pour le pirate. Et l'envoi de ce spam n'aura quasiment rien coûté…

« SUR L'AFFAIRE ASHLEY MADISON, IL Y AVAIT DES NOMS, DES ORIENTATIONS SEXUELLES, DES ÉVENTUELLES INFIDÉLITÉS ET DES COORDONNÉES BANCAIRES. CES QUATRE ÉLÉMENTS FONT QUE C'ÉTAIT UNE CIBLE PRÉVISIBLE »

→ LE SAVIEZ-VOUS [1] ?

• Selon l'institut eMarketer, le monde compte en 2015 quelques 3,07 milliards d'internautes. Et ils devraient être 3,6 milliards en 2018. Ce qui représente 48,2 % de la population mondiale.
• Selon l'estimation annuelle publiée par la société de cybersécurité Symantec, les cinq premiers pays dont seraient originaires les cyberattaques seraient : les Etats-Unis (20 %), la Chine (9,1 %), l'Italie (6 %), Taïwan (6 %) et le Brésil (5,7 %). Mais attention : l'origine géographique ne peut pas toujours être établie avec certitude. Et le fait de localiser les ordinateurs d'où sont parties les attaques, ne signifie pas que ceux-ci aient été utilisés avec l'accord de leur propriétaire légitimes ou l'assentiment des autorités de l'Etat en question.

(1) Extraits de *La cybersécurité. Mesurer les risques, organiser les défenses*, de Nicolas Arpagian.

« INTERNET N'EST EFFECTIVEMENT QU'UN OUTIL. UN MARTEAU PEUT SERVIR À CONSTRUIRE UNE MAISON… OU À FRACASSER LA TÊTE DE SON VOISIN »

LES ANONYMOUS SONT DES « HACKERS CITOYENS », DANS LA MESURE OÙ ILS DÉFENDENT DES CAUSES NOBLES ?
Ces pirates utilisent en effet les technologies informatiques et les réseaux sociaux dans des buts militants : dénonciation de la pédophilie, défense de la liberté d'expression, stigmatisation des régimes autoritaires… Le premier combat des Anonymous a été la lutte contre la scientologie. Ensuite, il y a eu des Anonymous qui ont commencé à révéler les coordonnées de personnes condamnées pour des faits de pédophilie. Est-ce bien ou non de le faire ? L'Eglise catholique a un gardien de la doctrine de la foi qui peut juger : « *Ceci est dans le dogme, ceci ne l'est pas* ». Pour les Anonymous, c'est moins le cas… L'autre problème c'est que vous pouvez tout à fait envoyer un communiqué, ou faire un compte Twitter en revendiquant que vous êtes un Anonymous…

VOUS VOULEZ DIRE QUE TOUT LE MONDE PEUT SE REVENDIQUER ANONYMOUS ?
Oui. Ce n'est pas une marque avec un cahier des charges précis. Il est très compliqué d'affirmer : « les Anonymous disent que » ou « les Anonymous font que ». On ne peut donc pas les concevoir comme une véritable entité.

MAIS LORSQUE CES HACKERS INTERNATIONAUX ONT TRAQUÉ ET SUPPRIMÉ QUELQUES SITES WEB FAISANT L'APOLOGIE DU DJIHAD, ÇA A ÉTÉ EFFICACE ?
C'est une contribution supplémentaire. Mais c'est forcément quelque chose d'éphémère. Car dès qu'un site disparaît un autre réapparaît. Chaque mois, il y a des comptes djihadistes qui ferment et d'autres qui ouvrent. D'autant que la grande force d'internet, c'est ce que l'on appelle « *la logique affinitaire* ».

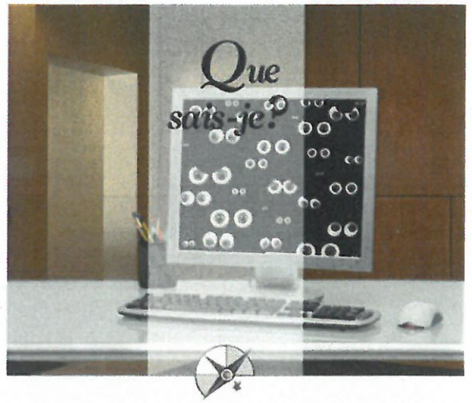
DE QUOI S'AGIT-IL ?
Si l'on ouvre un compte Facebook et que l'on poste des photos relatives au djihad ou à une certaine pratique de l'islam, l'algorithme de Facebook va faire venir à vous d'autres personnes ayant le même centre d'intérêt. Alors que vous ne les connaissez pas. Il suffit que vous ayez bien documenté votre page et l'algorithme fait le travail : « *Vous qui aimez ça, vous aimerez ça…* » Les distances géographiques s'abolissent et vous êtes liés par votre passion commune.

C'EST APPLICABLE À TOUTES LES MOUVANCES ?
Oui. Cela marche pour les djihadistes mais cela marche aussi pour les souverainistes, les complotistes, les sectes… Mais aussi, et heureusement, pour les personnes formidables qui ont des projets désintéressés… Toutefois, cette logique affinitaire est un peu sclérosante, car elle ne fait que réunir des gens qui ont déjà les mêmes centres d'intérêt.

EST-CE QUE DAESH UTILISE AUSSI LES CYBERATTAQUES ?
Bien sûr. Daesh a un grand avantage, c'est que ces individus ont de l'argent lié à la vente du pétrole. On peut tout à fait considérer qu'ils utilisent les services de « mercenaires numériques ». Ou alors, ils parviennent à convaincre des personnes à s'engager dans leur combat. Non pas en fournissant leur engagement physique, mais en partageant leur matière grise. L'avantage dans ce cas précis, c'est que ces personnes peuvent être disséminées partout géographiquement.

POUR DAESH, INTERNET EST AUSSI UNE REDOUTABLE ARME DE PROPAGANDE…
Il faut en effet distinguer les attaques informatiques et la prise de parole sur les réseaux sociaux. La propagande de Daesh est d'ailleurs très soignée : il y une scénarisation et une esthétique — même si c'est délicat d'utiliser ce terme-là — qui correspondent à ce que les gens ont de plus en plus l'habitude de voir. Avec des musiques, des vrais génériques, des fondus enchaînés…

INTERNET PEUT DONC PARAÎTRE COMME UN OUTIL ASSEZ EFFRAYANT…
Internet n'est effectivement qu'un outil. Un marteau peut servir à construire une maison… ou à fracasser la tête de son voisin. Une technologie, si on fait le parallèle religieux, est agnostique. Un outil n'est que ce que l'on en fait. C'est le comportement des humains qui est condamnable. Pas l'outil en lui-même.



LA CYBERSÉCURITÉ
Nicolas Arpagian
puf

« EN MATIÈRE D'ACTIVITÉ FINANCIÈRE, ON EST DANS DE L'ÉCONOMIE NUMÉRISÉE. L'EXPOSITION AUX RISQUES NUMÉRIQUES EN PRINCIPAUTÉ EST DONC RÉELLE »

COMME D'AUTRES PAYS, MONACO PEUT ÊTRE AUSSI LA CIBLE DE CYBERATTAQUES ?
Absolument. Dès que vous êtes connecté au réseau, vous êtes potentiellement une cible. Qu'il s'agisse d'un particulier, d'une entreprise ou d'un Etat. Monaco est donc évidemment une cible potentielle. Aujourd'hui, la finance et la bourse sont des marchés dématérialisés. Ce ne sont plus des individus qui s'échangent des papiers autour d'une corbeille avec des ordres d'achat et de vente griffonnés. En matière d'activité financière, on est dans de l'économie numérisée. L'exposition aux risques numériques en Principauté est donc réelle.

MONACO ENVISAGE DE CRÉER UNE AGENCE DE SÉCURITÉ NUMÉRIQUE, L'ÉQUIVALENT FRANÇAIS DE L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI) : C'EST INDISPENSABLE POUR UN PAYS ?
C'est un choix stratégique. Le rôle d'une agence gouvernementale comme l'ANSSI est d'assurer la sécurité des infrastructures étatiques et vitales d'un pays : à savoir le traitement des eaux, les institutions de santé, mais aussi les services de l'Etat. Dans le cas de Monaco, il s'agira du palais princier, du gouvernement, du Conseil national… Sa mission est donc de détecter les attaques informatiques 24h/24 et de prévenir les menaces. Dans ce type d'agence, il faut des cerveaux capables d'apprivoiser les technologies de plus en plus élaborées qui sont mises sur le marché par les grands équipementiers chinois ou américains par exemple.

LA CONVENTION DE BUDAPEST EST NÉE LE 23 NOVEMBRE 2001, MONACO L'A SIGNÉE EN MAI 2013 ET LE PROCESSUS DE RATIFICATION EST EN COURS AU CONSEIL DE L'EUROPE : C'EST TARDIF ?
Monaco a mis en effet une douzaine d'années à signer ce texte. Ce qui est, certes, beaucoup… Mais le processus a été tardif pour de nombreux grands pays. Plusieurs pays européens comme Andorre, la Grèce, l'Irlande ou encore la Suède ne l'ont toujours pas ratifié. Or, sans ratification, un pays n'a pas d'obligation de le transposer dans son droit national. Signer n'engage à pas grand chose. Ce qui engage, c'est la ratification et la date d'entrée en vigueur.

LE TEMPS ENTRE LA SIGNATURE ET LA RATIFICATION PEUT DONC AUSSI ÊTRE TRÈS LONG…
Absolument. L'Allemagne par exemple a signé le texte — comme la majorité des grands pays — en novembre 2001, mais a attendu mars 2009 pour le ratifier. Le texte est entré en vigueur dans le droit allemand en juillet 2009. En revanche, il y a des pays comme Saint-Marin et la Russie qui n'ont toujours pas jugé utile d'y apposer leur signature.

QUELLE EST L'ORIGINE DE CETTE CONVENTION ?
Cette convention de Budapest qui date de novembre 2001, n'est pas ce que j'appelle « un enfant du 11 septembre » contrairement au Patriot Act américain qui, lui, a été élaboré et adopté suite aux attentats de New York. C'est une convention internationale qui était en gestation avant le 11 septembre et qui avait notamment comme ambition de lutter contre la pédopornographie sur internet. C'est donc difficile pour un pays de s'afficher contre une telle convention. Historiquement, le pays a envie d'être sur la photo de la famille. Il y a donc une sorte de consensus de façade pour dire qu'il faut coopérer…

ET AUJOURD'HUI ?
C'est le principal texte de dimension internationale en matière de criminalité numérique. Il oblige notamment un pays à adapter son droit national et à prévoir des infractions spécifiques au cybercrime. Il oblige à coopérer ou encore à établir un système de preuve.

bonarrigo@monacohebdo.mc
@sabrinabonarigo

(1) *La cybersécurité. Mesurer les risques, organiser les défenses* de Nicolas Arpagian (Editions Presses universitaires de France (PUF), collection Que sais-je ?), 127 pages, 9 euros.