monaco HEBDO
27 BOULEVARD D'ITALIE
98000 MONACO - 00 377 93 50 56 52

28 OCT/03 NOV 10
Hebdomadaire Province

Surface approx. (cm²) : 5329

monaco HEBDO
27 BOULEVARD D'ITALIE
98000 MONACO - 00 377 93 50 56 52

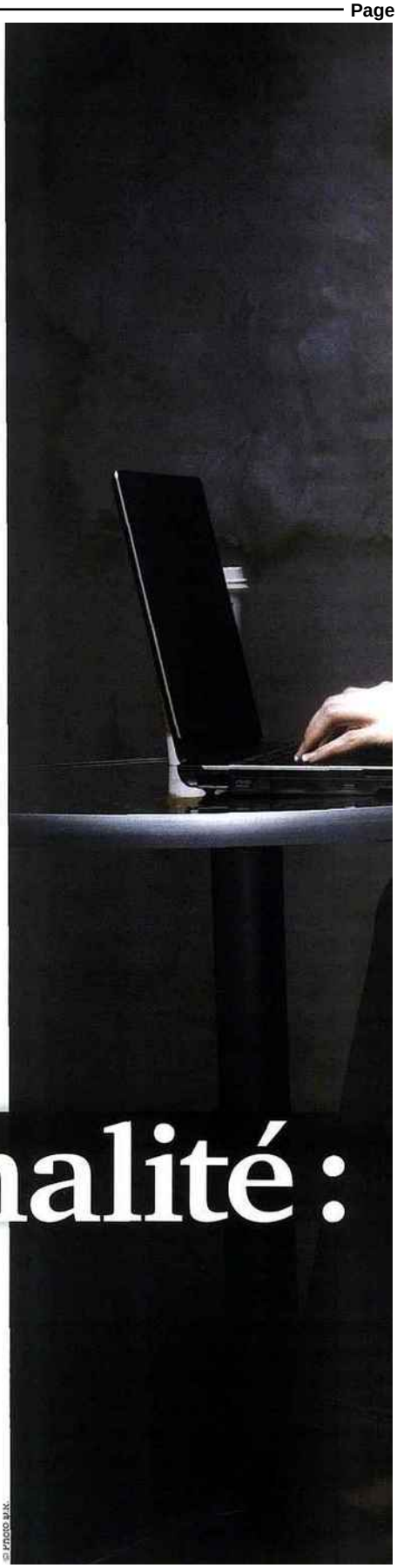
28 OCT/03 NOV 10
Hebdomadaire Province

Surface approx. (cm²) : 5329

Cybercriminalité :

Etat, particuliers ou entreprises sont tous des victimes potentielles de cyberattaques sur Internet. Un danger d'autant plus réel pour les internautes monégasques. Car l'arsenal juridique en matière de cybercriminalité est quasi inexistant.

Par Sabrina Bonarrigo.



Données bancaires, déclaration d'impôts ou vie privée étalée sur des réseaux sociaux… Des pans entiers de notre existence sont aujourd'hui livrés à Internet. Un espace numérique avec son lot d'escroqueries en tous genres. Fraude à la carte bleue, encaissement de paiement sans livraison de marchandise, vente par petites annonces ou aux enchères d'objets volés et contrefaits. Sans oublier la diffusion d'images pédophiles ou d'injures à caractère racial. La palette des infractions possibles sur le Web est large et très difficile à chiffrer (lire interview p. 32). Des attaques logiquement exponentielles. *« Le risque est aujourd'hui multiplié par trois. Car on est à la fois connecté à son travail, à son domicile et sur son mobile »*, explique Nicolas Arpagian, rédacteur en chef de la revue *Prospective stratégique*. Le monde virtuel serait d'ailleurs passé d'un réseau de 400 millions d'internautes à près de 2 milliards d'usagers en 10 ans. Un bilan effectué lors de la 10ème édition des Assises de la sécurité qui se sont tenues en octobre à Monaco. Une décennie durant laquelle les ordinateurs ont été envahis par des campagnes de spam, de phishing et autres déluges de chevaux de Troie. Et sur les attaques cybernétiques, les spécialistes sont formels : le risque zéro n'existe pas.

PAS DE LÉGISLATION À MONACO

Monaco n'échappe pas à la règle. Pas moins de 14 000 résidents sont aujourd'hui connectés à Internet (1). Et en cas de fraude sur la Toile, c'est à la sûreté publique que les victimes doivent se rendre. 186 plaintes pour usage frauduleux de numéro de carte bancaire sur Internet ont d'ailleurs été enregistrées en 2009. *« Pour la période considérée en 2010, nous enregistrons une légère baisse. Il n'y a pas eu en revanche de plainte pour usurpation numérique d'identité »*, précise la sûreté publique. Et si ces escroqueries sont très sévèrement punis en France (5 ans maximum d'emprisonnement et une amende de 375 000 euros maximum), a contrario, en matière de cybercriminalité à Monaco, c'est un vrai no man's land juridique. Aucun arsenal ne protège réellement les internautes. *« Ces textes sont attendus depuis longtemps puisqu'ils ont été demandés par le Conseil de l'Europe au moment de l'adhésion de Monaco. La principauté s'était engagée à prendre un certain nombre de dispositions législatives. A ce jour, il n'y a rien. Seuls les actes de pédophilie sur Internet sont heureusement incriminés pour protéger les mineurs. Il n'y a donc pas d'incriminations spécifiques à Monaco permettant de lutter contre la cybercriminalité,* explique un juriste. *Quand une personne est victime*

monaco HEBDO
27 BOULEVARD D'ITALIE
98000 MONACO - 00 377 93 50 56 52

28 OCT/03 NOV 10
Hebdomadaire Province

Surface approx. (cm²) : 5329

monaco HEBDO
27 BOULEVARD D'ITALIE
98000 MONACO - 00 377 93 50 56 52

28 OCT/03 NOV 10
Hebdomadaire Province

Surface approx. (cm²) : 5329

Pédopornographie : Monaco Télécom en gendarme de la Toile

5 550 tentatives d'accès à des sites pédopornographiques ont été enregistrées d'avril 2009 à juillet 2010 par Monaco Télécom. Depuis plus d'un an, l'opérateur monégasque exerce un système de filtrage pour bloquer l'accès aux sites à contenu pédopornographique. Notamment grâce à une veille technologique. La stratégie consiste à exercer une veille régulière de sites « P2P » avec un logiciel qui cherche à n'importe quel moment du jour et de la nuit et de manière automatique, des traces de détection de pédopornographie. Le système est en exploitation au sein de la section des mineurs et protection sociale (SMPS) en collaboration avec l'association Action Innocence, elle-même partenaire avec une association anglaise Internet Watch Foundation qui effectue des mises à jour quotidiennes des nouveaux sites recensés. Ce projet a d'ailleurs reçu le prix Francopol sur la cybercriminalité. Il constitue un véritable outil pour la police monégasque. « *5 condamnations ont été prononcées en 2009 pour téléchargement de fichiers pédopornographiques* », explique Christophe Andronaco, chef de section à la SMPS. Reste à combler les lacunes sur toutes les autres infractions virtuelles.

◀ Pas moins de 14 000 résidents sont aujourd'hui connectés à Internet. Et en cas de fraude sur la Toile, c'est à la sûreté publique que les victimes doivent se rendre.

© Photo D.R.

par exemple d'une fraude à la carte bleue sur Internet, l'usager doit donc saisir sa banque, prouver qu'elle a été victime d'une fraude et la banque rembourse. » Excepté, en matière de pédopornographie, le déficit législatif est donc réel.

PAS DE NOUVELLES ATTAQUES 100 % INTERNET

Selon les spécialistes, la Toile ne regorge pas en revanche de nouvelles infractions « 100 % Internet ». « *Les activités cybercriminelles sont des délits que l'on connaît déjà dans le code pénal classique : le vol, l'extorsion, le chantage ou encore la diffamation* », rajoute Nicolas Arpagian. Mais c'est son impact qui change. « *Par exemple, une diffamation dans un village, reste dans le village. Sur Internet, elle prend une dimension internationale. Sa circulation est beaucoup plus rapide, et en pratique, ça ne coûte pas grand chose au pirate* », explique le spécialiste. Autre changement notoire : la permanence. Sur Internet, la diffamation dure inexorablement dans le temps. Bien que la notion de « droit à l'oubli » commence concrètement à faire son chemin (voir encadré).

La pédagogie, elle, en revanche, est en ordre de marche. Y compris à Monaco. « *Nous allons lancer prochainement une campagne d'information sur les dangers de l'utilisation inconsidérée des réseaux sociaux, sur l'utilisation du cloud computing*(2) *sur la géolocalisation ou encore sur la biométrie* », explique Michel Sosso, président de la Commission de contrôle des informations nominatives (CCIN), qui n'hésite pas à parler de « *danger dans notre intimité.* » Exemple : la CNIL (Commission nationale de l'informatique et des libertés) a récemment mis en garde les internautes sur les dangers de la géolocalisation initiée par Facebook dans un avis publié sur son site Internet. Baptisé « Facebook places », ce dispositif lancé le 30 septembre en France permet aux membres du réseau de partager avec leurs amis des informations sur les lieux où ils se trouvent et de savoir quels amis se trouvent à proximité. « *Publier sa localisation au cours de la journée peut conduire à dévoiler aux cambrioleurs potentiels vos horaires de présence ainsi que votre adresse* », cite en exemple la CNIL qui invite les internautes à la « *plus grande prudence* » notamment sur les paramètres de confidentialité.

186 plaintes pour usage frauduleux de numéro de carte bancaire sur Internet déposées à la sûreté publique en 2009

Autre avertissement pour l'internaute : « *70 % des DRH, lors d'un recrutement, regardent d'abord les profils sur Facebook* », rappelle Michel Sosso.

La pédagogie semble salutaire aussi dans les écoles. Alors qu'en France la CNIL va consacrer 500 000 euros à la sensibilisation des enseignants et des élèves, l'association Action innocence continue de son côté le

monaco HEBDO
27 BOULEVARD D'ITALIE
98000 MONACO - 00 377 93 50 56 52

28 OCT/03 NOV 10
Hebdomadaire Province

Surface approx. (cm²) : 5329

70 % des DRH, lors d'un recrutement, regardent d'abord les profils sur Facebook

même travail à Monaco. En expliquant notamment aux parents et élèves les nouveaux risques qui émergent. A l'image du chatroulette, un visiochat mettant en contact des internautes de manière aléatoire. Autant de phénomènes qui échappent souvent aux parents.

FOSSÉ GÉNÉRATIONNEL

Difficile parfois pour les plus anciennes générations de capter les subtilités et les dangers du monde numérique. « *Notre système d'éducation a toujours été historiquement fondé sur le principe du compagnonnage. Ce sont les anciens qui transmettent aux jeunes générations. Le problème avec les technologies d'Internet, c'est que l'on inverse le processus. Les personnes dites « responsables » sont en peine pour faire de la pédagogie, voire exercer une autorité sur les plus jeunes. Les personnes qui ne maîtrisent pas les réseaux sociaux ne peuvent pas imaginer tout ce qui est potentiellement dangereux* », explique Nicolas Arpagian. Les acteurs du secteur inventent d'ailleurs toujours de nouvelles fonctionnalités, comme la géolocalisation par Facebook ou Twitter. Difficile ainsi de se prémunir face à un domaine qui est très mouvant. D'autant plus que la dématérialisation de la société touche à présent tous les domaines: de l'e-commerce à l'e-business. En passant par l'e-administration ou encore l'e-santé. Un monde virtuel dans lequel les infractions en revanche sont bien réelles. « *A Monaco, les gens sont encore très peu sensibilisés à ces problèmes. Mais la première protection vient de soi. En sachant limiter, ce que l'on indique comme élément de sa vie privée sur Internet. Tout le monde pense par exemple qu'une fois le profil sur Facebook effacé, les données sont oubliées et sortent du réseau. Mais c'est faux* », alerte Michel Sosso. L'internaute doit donc être son premier garde-fou face à la cybercriminalité. « *Contrairement à des activités comme la chasse ou la conduite où un permis est nécessaire au nom de la sécurité, sur Internet, chacun doit singulièrement se sécuriser via des logiciels payants ou gratuits. On transfère donc la responsabilité de la sécurisation à l'utilisateur final. Il n'y a pas d'équivalent* », précise Nicolas Arpagian. Dans les entreprises, la sécurité informatique est également de la responsabilité propre de chaque société. Le CHPG par exemple a renforcé sa protection en recrutant depuis 2 ans, une personne qui consacre une partie de son temps à la fonction de « RSSI »: responsable sécurité du système d'information. ■

(1) Chiffres de Monaco Télécom. Alors que 20 millions de Français sont connectés à l'Internet en haut débit.
(2) Le cloud computing est un programme qui permet grâce à une connexion Internet, d'externaliser un certain nombre de ressources informatiques.

De Mafiaboy au virus I love you

Depuis l'explosion d'Internet plusieurs cyberattaques ont défrayé la chronique et fait la Une des médias. Parmi elles, l'affaire Mafiaboy en mai 2000. En pleine bulle Internet, un adolescent canadien de 15 ans crée un bombardement électronique sur les sites d'Amazon, e-Bay ou encore Yahoo. Le jeune pirate est arrêté par le FBI. Il sera condamné à des travaux d'intérêt général et interdit d'utilisation d'un ordinateur pendant 2 ans. Quelques mois plus tard, un courriel au titre pour le moins intriguant « *Je vous aime* » venu des Philippines en mai 2000 incite les Internautes à ouvrir une pièce jointe. Le message contient un virus (un ver) dont la principale fonctionnalité est de renvoyer le message d'origine à tout le carnet d'adresse du destinataire. Effet boule de neige immédiat. L'attaque infectera plus de 3 millions d'ordinateurs en seulement 4 jours. Un jeune étudiant en informatique philippin est épinglé mais il restera impuni car les Philippines n'ont pas de loi contre le piratage informatique. Autre attaque d'envergure: en avril 2010, un pirate nommé « Kirlos » propose à la vente plus de 1,5 millions de données personnelles volées, issues de Facebook, pour un prix allant de 25 à 45 dollars pour 1 000 contacts.

Un droit à l'oubli boudé par Facebook et Google

Le chantier n'est pas une mince affaire: garantir un droit à l'oubli numérique aux internautes. Un pas semble avoir été récemment franchi en la matière. Une douzaine de signataires, réunis par Nathalie Kosciusko-Morizet, secrétaire d'Etat chargée de la prospective et du développement de l'économie numérique en France, ont adopté, le 13 octobre dernier à Paris, une charte consacrée au droit à l'oubli numérique. Objectif: mettre en place de nouveaux dispositifs afin de garantir la protection des données privées des internautes. Parmi les signataires figurent la plate-forme de blogs Skyblog et ses 40 millions d'inscrits. Ou encore les services Pages jaunes et le site « Copainsdavant ». Sur le banc des absents en revanche, les géants Google et Facebook. Pour les réseaux sociaux, ce droit à l'oubli consisterait à créer un « bureau des réclamations » virtuel qui permettrait de centraliser les demandes de modification ou de suppression d'un compte. Les moteurs de recherche devraient, de leur côté, supprimer le cache des pages indexées. Notamment quand les contenus supprimés figuraient sur les réseaux sociaux.

▲ La CNIL a récemment mis en garde les internautes sur les dangers de « Facebook places ».

monaco HEBDO
27 BOULEVARD D'ITALIE
98000 MONACO - 00 377 93 50 56 52

28 OCT/03 NOV 10
Hebdomadaire Province

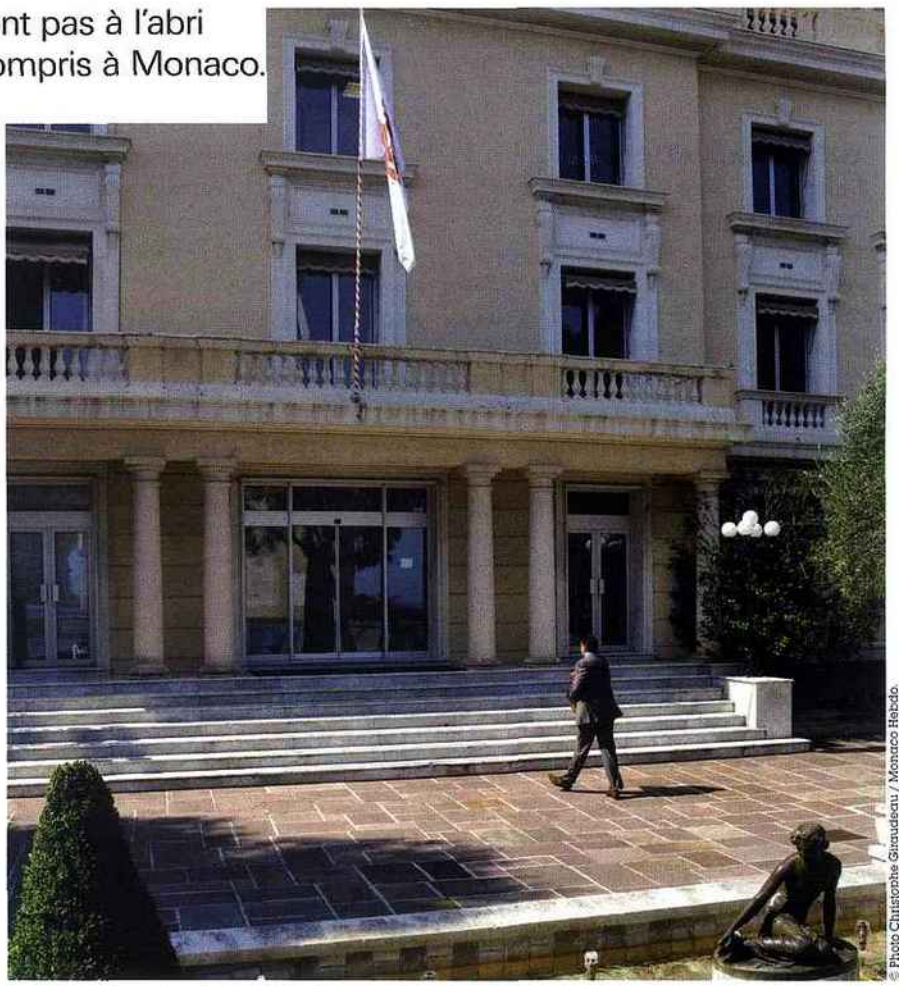
Surface approx. (cm²) : 5329

"CYBERGUERRE" : quels risques pour Monaco ?

Gouvernements et Etats ne sont pas à l'abri d'attaques cybernétiques. Y compris à Monaco.

Par Sabrina Bonarrigo.

Guerre informatique, cyberdélinquance ou cyberguerre… Depuis l'avènement d'Internet, toute une sémantique s'est créée autour des conflits et des délits provenant d'Internet. Et les exemples de cyberattaques sont multiples. Désinformation, propagande, défiguration de pages web, informations confidentielles interceptées et modifiées, arrêt ou sabotage d'équipements… Autant d'attaques dont Etats et gouvernements peuvent être des victimes directes (voir interview page 32). Monaco, comme les autres pays, n'est donc pas à l'abri. *« Le canon peut être parfaitement orienté sur Monaco. Dans la mesure où nous sommes dans une économie dématérialisée, des données peuvent être détournées. Une banque ou une société peut faire l'objet d'une attaque ciblée*, explique Nicolas Arpagian qui estime *qu'une attaque peut être aussi d'ordre plus politique. On pourrait tout à fait envisager que dans une logique militante ou politique, certains, notamment des alter mondialistes, puissent s'attaquer au symbole de luxe et d'opulence que la principauté représente. Aller porter le fer jusqu au cœur de l'argent peut être un symbole fort ».*



© Photo Christophe Gruudeau / Monaco Hebdo

▲ ***« A ce jour, les dispositifs de sécurité mis en place par le service informatique de l'Etat n'a jamais été pris en défaut »*, selon le service informatique du gouvernement.**

ENNEMIS INVISIBLES

Pour les Etats, le vice sous-jacent sur Internet est que les assaillants sont par définition invisibles. *« Les Etats ou les industriels ont des ennemis héréditaires, bien identifiés. Par exemple, le groupe Areva a Greenpeace comme ennemi héréditaire. Or avec Internet il y a des ennemis que l'on n'avait pas détecté sur les écrans radars, qui peuvent arriver de toute part. Ce qui oblige à une veille et une anticipation constantes »*, ajoute le spécialiste. La principauté a-t-elle alors été déjà menacée par des attaques informatiques ? *« A ce jour, les dispositifs de sécurité mis en place par le service informatique de l'Etat n'a jamais été pris en défaut »*, explique le service informatique du gouvernement. Si Monaco ne dispose pas

Dans une logique politique ou militante, des alter mondialistes, pourraient s'attaquer au symbole de luxe et d'opulence que la principauté représente.

monaco HEBDO
27 BOULEVARD D'ITALIE
98000 MONACO - 00 377 93 50 56 52

28 OCT/03 NOV 10
Hebdomadaire Province

Surface approx. (cm²) : 5329

de réelle cellule spécifique à l'instar de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France, 28 personnes au total assurent une cyberdéfense de l'Etat. Une cybersécurité assurée à la fois de manière « *préventive et proactive* ». Objectif: éviter les intrusions éventuelles et les tentatives de piratage. Le gouvernement affiche ainsi un argumentaire très technique et détaillé pour expliquer la politique de défense de son cyberespace.

SYSTÈME DE PROTECTION

La protection du réseau monégasque est d'abord assurée par un double niveau de système protecteur dit « firewall » qui concerne à la fois les sites web consultés par les internautes [1], la navigation depuis les postes utilisateurs vers l'externe ainsi que les journaux d'activités. Un système de filtrage des mails a également été mis en place pour les messages échangés avec l'extérieur. Avec des solutions de type « anti-spam », « anti-virus » et « anti-spyware ». Le gouvernement est d'ailleurs son propre hébergeur pour les serveurs de mails. A noter également qu'un « firewall » a été mis en place pour les connexions avec les principales entités publiques telles que la police, les services judiciaires, les parkings publics ou encore la mairie. « *Des serveurs redondants sont parallèlement installés dans la salle machine sécurisée du gouvernement. Ils comprennent des disques « en miroir », avec présence d'un doublon physique pour chacun d'eux en salle de secours. Depuis 2005, on utilise des technologies de « virtualisation ». Cela entraîne une diminution significative du nombre de serveurs physiques. A ce jour, il y a plus de 60 serveurs virtuels hébergés sur 4 serveurs physiques* » explique encore le service. Cette « salle de secours », comme sa dénomination le suggère, permet un redémarrage des activités informatiques en cas de « catastrophe » de quelque nature que ce soit sur le site principal. Et des alertes téléphoniques ou via mail préviennent les techniciens en cas de défaillances.

Pas de Wi-fi sur le réseau du gouvernement afin d'éviter d'éventuelles intrusions

POSTES DE TRAVAIL SÉCURISÉS

Les postes de travail des fonctionnaires et agents de l'Etat sont également sécurisés par différents dispositifs. Notamment une carte à puce qui protège l'accès au poste de travail et aux données administratives personnelles ainsi qu'un contrôle sur l'accès aux bâtiments. « *En plus de l'antivirus sur les serveurs de messagerie, un antivirus est installé localement afin de se protéger des risques des clés USB ou autre support amovible* », explique encore le service informatique. Autre garde-fou: pas de Wi-fi sur le réseau du gouvernement afin d'éviter d'éventuelles intrusions. ■

(1) Y compris les usagers pour tout ce qui touche aux télé-procédures.

BlackBerry: une utilisation polémique

Ces téléphones conçus à l'origine pour les hommes d'affaires se retrouvent désormais largement entre les mains de politiques, y compris monégasques, et de particuliers. Un téléphone dont l'usage a pourtant fait polémique. « *En 2005 le secrétariat général de la défense nationale en France avait déconseillé aux équipes gouvernementales d'utiliser le BlackBerry car l'intégralité des données qui passent par cet appareil est obligée de passer par des serveurs Research in motion (RIM), du nom de l'entreprise qui a crée BlackBerry. Donc potentiellement cette entreprise voit passer l'intégralité des communications véhiculées par BlackBerry. Il pouvait donc y avoir des doutes sur l'intégrité des données* », explique Nicolas Arpagian. Début août, c'est Berlin qui déconseille à son tour aux équipes ministérielles l'usage des téléphones BlackBerry et Iphone Apple au nom des menaces qu'ils représentent en terme de sécurité. Illustration selon le spécialiste de « *la dépendance technologique dans laquelle se trouvent désormais les Etats à l'égard de quelques opérateurs commerciaux* ».

monaco HEBDO
27 BOULEVARD D'ITALIE
98000 MONACO - 00 377 93 50 56 52

28 OCT/03 NOV 10
Hebdomadaire Province

Surface approx. (cm²) : 5329

Nicolas Arpagian, rédacteur en chef de la revue *Prospective stratégique* et coordonnateur d'enseignements à l'Institut national des hautes études de la sécurité et de la justice (INHESJ), analyse les différents risques cybernétiques auxquels sont confrontés les Etats.

Propos recueillis par Sabrina Bonarrigo.

"L'Etat est aussi vulnérable que les autres"

Monaco hebdo: Concrètement, que recouvre le terme de « cyberguerre » dont vous parlez dans l'un de vos ouvrages [1]?

Nicolas Arpagian: Le terme cyberguerre est l'utilisation des technologies de l'information, et donc d'Internet, à des fins offensives. Par exemple, faire en sorte de contaminer le système informatique d'une administration, d'une armée, d'une entreprise, d'un particulier ou d'une institution. L'espionner, en interceptant des informations. Cela peut consister aussi à prendre le contrôle d'une machine pour interrompre son fonctionnement. On peut également altérer des données. Comme ce collégien de 5ème du nord de la France qui voulait changer ses notes du 3ème trimestre. Comme il n'y est pas parvenu, il a fait une campagne de spam et fait tomber l'informatique du collège pendant une semaine. Dans un système militaire, étant donné que les armes sont de plus en plus géolocalisées, cela peut consister également à dérégler des systèmes de contrôle. Au lieu de tirer sur la base militaire, on décale le tir sur un orphelinat. Pour ensuite utiliser les images de cet orphelinat bombardé comme un élément d'influence politique. L'étape ultime de ces attaques, est de faire en sorte que le système de votre adversaire ne fonctionne plus du tout.

M.H.: D'autres exemples?

"Des sites gouvernementaux géorgiens ont fait l'objet de cyberattaques durant l'été 2008, avec leurs pages d'accueil remplacées par des portraits d'Adolf Hitler"

N.A.: Sur Internet, il est possible aussi de mener des campagnes de dénigrement en rendant disponibles des informations sur telle ou telle entreprise, ou tel ou tel individu, pour lui porter préjudice. Ou inversement, faire en sorte qu'une information ne soit plus accessible. Une attaque informatique peut être aussi une manière pour un adversaire de montrer son pouvoir. Les sites gouvernementaux géorgiens par exemple ont fait l'objet de cyberattaques durant l'été 2008, avec notamment leurs pages d'accueil remplacées par des portraits d'Adolf Hitler. Il ne s'agissait pas de dire que le gouvernement géorgien est nazi. Mais plutôt : *« Moi assaillant je peux rentrer chez vous et prendre le contrôle de vos organisations. »* Dans ces cas-là, le message est aussi destiné à l'opinion publique du pays. Pour faire comprendre : *« Votre gouvernement n'est pas capable d'assurer la sécurité informatique de son Etat ».*

M.H.: Entreprises, particuliers ou Etat, qui est le plus vulnérable face aux attaques informatiques?

N.A.: L'année dernière le compte bancaire personnel de Nicolas Sarkozy a été piraté. Les pirates ont été arrêtés. On lui a volé plusieurs centaines d'euros. Je suis convaincu que si les pirates avaient su que parmi les comptes piratés il y avait celui du président, ils n'y auraient pas touché. Car très rapidement, il y a eu tout un déploiement policier et judiciaire pour les trouver qu'il n'y aurait pas eu si c'était un « anonyme ». Mais cette affaire montre que la taille de l'entité, la nature de l'activité ou la localisation géographique ne protège pas d'une attaque. A partir du moment où l'on est connecté au réseau, on est tous des victimes potentielles. On peut faire certes l'objet d'une attaque ciblée. Mais on peut être aussi pris dans de vastes filets qui contamineront plusieurs centaines de milliers d'ordinateurs. Par exemple, en 2008, les ordinateurs du Minis-

monaco HEBDO
27 BOULEVARD D'ITALIE
98000 MONACO - 00 377 93 50 56 52

28 OCT/03 NOV 10
Hebdomadaire Province

Surface approx. (cm²) : 5329

***« La taille de l'entité, la nature de l'activité ou la localisation géographique ne protège pas d'une attaque. A partir du moment où l'on est connecté au réseau, nous sommes tous des victimes potentielles »,* Nicolas Arpagian. ▶**

© Photo D.R.

tère français de la défense ont fait partie des victimes du ver Conficker qui a frappé des milliers d'ordinateurs fonctionnant sous Windows. L'Etat est donc aussi vulnérable que les autres.

M.H.: Existe-t-il justement des chiffres sur la cybercriminalité?

N.A.: Il n'existe pas vraiment de statistiques. Hormis celles qui émanent des éditeurs de logiciel de sécurité. Comme Symantec ou encore Trend Micro. Ces éditeurs livrent pléthore de chiffres par région et par période. Mais il est évident qu'il n'est pas bon que celui dont le travail est de vendre des systèmes de sécurité dévoile des statistiques. En termes de fiabilité, d'intégrité et d'indépendance, c'est discutable. La cybercriminalité est donc très difficile à mesurer. Pour plusieurs raisons. Soit parce que l'on n'est pas conscient que l'on est attaqué. Soit parce qu'une entreprise attaquée ne le révélera pas. Pour éviter que cela ne porte atteinte au crédit ou à l'image de l'entreprise. La mesure à laquelle je crois en revanche est d'obliger les entreprises, notamment par le biais des commissaires au compte, à le notifier dans leur bilan lorsqu'ils font l'objet d'une attaque.

"Barack Obama a parallèlement indiqué que la prospérité des Etats-Unis passait par la cybersécurité"

Quitte à ce que ce chiffre reste confidentiel au public. Mais il faut que les services de l'Etat puissent avoir au minimum un chiffre agrégé par taille et par secteur d'activité. Les Etats-Unis ont en revanche un baromètre de la cybersécurité appelé le « Internet crime compliant center ». Chaque année, ce centre publie les statistiques des plaintes déposées relatives à des fraudes sur le Net, avec la collaboration du FBI. C'est un indicateur instructif pour suivre l'évolution des cyberattaques. Mais dans ces chiffres, ne sont évidemment pas prises en compte les victimes qui n'en n'ont pas conscience. Sans oublier tous les cas où celles-ci ne veulent pas porter plainte.

M.H.: Comment se protègent la France et les autres pays?

N.A.: La cyberdéfense de l'Etat français est assurée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Son rôle est d'assurer la protection informatique des infrastructures de l'Etat et d'être un conseil pour les infrastructures critiques vitales du pays. De type eau, énergie, électricité ou transports. Son deuxième travail consiste à labelliser des solutions de sécurité. En clair, un éditeur qui a élaboré un logiciel de sécurité le présente à l'ANSSI. L'agence va alors tester sa robustesse et lui attribuer un label. Les Allemands ont en revanche une toute autre approche. Une agence spécifique développe ses propres solutions et il les vend aux administrations et aux infrastructures vitales. C'est un système qui rapporte de l'argent et qui permet donc de mieux payer les ingénieurs et de recruter des experts très qualifiés. Dans un discours en mai 2009 Barack Obama a parallèlement indiqué que la prospérité des Etats-Unis passait par la cybersécurité. Il a également demandé la collaboration des entreprises américaines. L'Etat n'est donc pas seul à la manoeuvre pour se défendre. Une entreprise comme Google va être considéré par la Chine comme un partenaire qui a le poids d'un Etat concernant le filtrage des données par exemple. Au nom de la sécurité, les Etats associent donc souvent les entreprises. ■

(1) Auteur de *L'État, la peur et le citoyen* (Vuibert 2010), de *Cybersécurité* (Que sais-je, 2010) et de *La cyberguerre* (Vuibert, 2009).

monaco HEBDO
27 BOULEVARD D'ITALIE
98000 MONACO - 00 377 93 50 56 52

28 OCT/03 NOV 10
Hebdomadaire Province

Surface approx. (cm²) : 5329

Sentinelle informatique

A l'instar de la CNIL française, la commission de contrôle des informations nominatives (CCIN), veille à ce que les données informatiques personnelles des résidents monégasques soient protégées. Une entité encore peu connue du grand public.

Par Sabrina Bonarrigo.

Le géant californien Google et son « street view » a récemment débarqué à Monaco. Dans moins de 6 mois, les Internautes pourront arpenter virtuellement les rues monégasques. Et en coulisses, c'est la CCIN (1) qui veillera notamment à ce que le floutage du visage des individus et des plaques d'immatriculation soit bien effectué. Cette autorité, pour l'heure très discrète, a pourtant été sur le devant de la scène lors du sondage mené par le trio d'experts français sur l'image de Monaco en mars dernier. Via un communiqué officiel publié dans la presse, la commission est montée au créneau pour dénoncer certains manquements dans la procédure (2). « *Le sondage n'a pas été soumis en amont à la CCIN comme le prévoit la loi. La commission n'a donc pas pu garantir la protection des informations et la confidentialité des réponses des personnes interrogées* ». En clair, le sondage aurait dû faire l'objet d'un avis en amont. Objectif : vérifier notamment qu'il n'y avait pas de questions liées à l'ethnie ou à la religion dans le sondage. Savoir également que deviendraient les informations traitées et si elles étaient anonymisées. Après l'avertissement de la CCIN, l'Etat rectifie le tir. « *La CCIN a réclamé à la société de sondage d'envoyer une attestation à l'Etat mentionnant que toutes les informatives nominatives recueillies lors du sondage ont bien été détruites. Ce qui a été fait* », précise le président.

▲ **Le géant californien Google et son « street view » a récemment débarqué à Monaco. Dans moins de 6 mois, les Internautes pourront arpenter virtuellement les rues monégasques.**

PLAINTES ET MISES EN DEMEURE

L'objectif premier de la CCIN est donc de protéger les données personnelles informatiques des individus contre tout abus. Une entité qui a toute sa raison d'être dans un univers de plus en plus numérisé et où la prolifération de fichiers automatisés, leur interconnexion, leur exploitation et leur conservation peuvent entraîner un risque d'utilisation abusive ou détourné. D'ailleurs depuis l'entrée en vigueur de la nouvelle loi (3), la CCIN a été saisie de quatre plaintes. Trois à l'encontre de sociétés monégasques et une contre l'Etat. « *Celle contre l'Etat concernait la plainte*

monaco HEBDO
27 BOULEVARD D'ITALIE
98000 MONACO - 00 377 93 50 56 52

28 OCT/03 NOV 10
Hebdomadaire Province

Surface approx. (cm²) : 5329

« Cinq responsables ont été mis en demeure de cesser l'exploitation de fichiers illégaux », indique Michel Sosso, président de la CCIN. ►

© Photo Monaco Hebdo.

d'un étranger. Son nom apparaissait sur Internet dans le journal officiel en ligne avec des informations personnelles le concernant. La CCIN est intervenue et a demandé à l'Etat de faire anonymyser le nom », rappelle Michel Sosso.

Autre rôle de la CCIN : garantir un droit d'accès aux individus qui souhaiteraient connaître le contenu des informations qui les concernent dans les fichiers publics ou privés. Un rôle d'intermédiaire que la CCIN a déjà rempli à deux reprises. Deux résidents français ont porté plainte contre une société monégasque qui leur avaient refusé un droit d'accès à leur dossier et un droit de rectification.

D'ailleurs si vous souhaitez savoir s'il y a des informations qui vous concernent à la sûreté publique, la CCIN est encore une fois l'intermédiaire à saisir. Un droit baptisé « d'accès indirect » sur un fichier de police. *« La personne intéressée peut alors saisir la commission qui fait procéder par un membre de la commission à la vérification demandée et aux modifications nécessaires si besoin »*, précise Michel Sosso. En cas d'irrégularité, la CCIN est aussi en droit de formuler avertissements et autres mises en demeure. *« Cinq responsables ont été mis en demeure de cesser l'exploitation de fichiers illégaux. Trois mesures de ce types ont été prononcées à l'égard de sociétés chargées de mission de service public. Une était destinée à une société privée. Une autre au ministre d'Etat pour une irrégularité constatée dans un service »*, rajoute Michel Sosso.

3 ANS D'ADAPTATION

Mais l'un des premiers rôles de la CCIN, plus administratif, reste de recenser les fichiers informatiques du secteur public et privé. En clair, recevoir les dossiers de déclaration, demande d'avis ou d'autorisation. Aujourd'hui 2 173 dossiers dont 873 cette année ont été déposés à la CCIN. Mais la commission reste pour l'heure encore dans une phase de *« rodage »*. *« Le temps d'adaptation pour un fonctionnement normal des CNIL est d'environ 3 ans. On est en train de s'installer. L'information aujourd'hui n'est pas suffisante pour appliquer avec rigueur les pénalités prévues par la loi. On est donc aujourd'hui plus tolérant »*, explique son président Michel Sosso. La tolérance sera moins de mise en revanche quand la campagne d'information sera lancée en début d'année prochaine. ■

(1) CCIN est une autorité administrative indépendante composée de 6 membres proposés au prince par différentes institutions (conseil national, ministre d'état, conseil d'Etat, conseil communal le conseil économique et social et le directeur des services judiciaires) nommés pour 5 ans.

(2) La CCIN doit être consultée par le Ministre d'état lors de l'élaboration de mesures législatives ou réglementaires relatives à la protection des droits et libertés des personnes à l'égard du traitement des informations nominatives. Le CCIN doit dénoncer au procureur général les faits constitutifs d'infraction et peut ester en justice. La nouvelle loi prévoit dans ses articles des sanctions lourdes allant de 3 mois à 1 an d'emprisonnement et une amende pouvant aller de 9 000 euros à 90 000 euros

(3) La loi sur la protection des informations nominatives est entrée en vigueur le 1er avril 2009. La nouvelle commission est entrée en vigueur en juillet 2009.