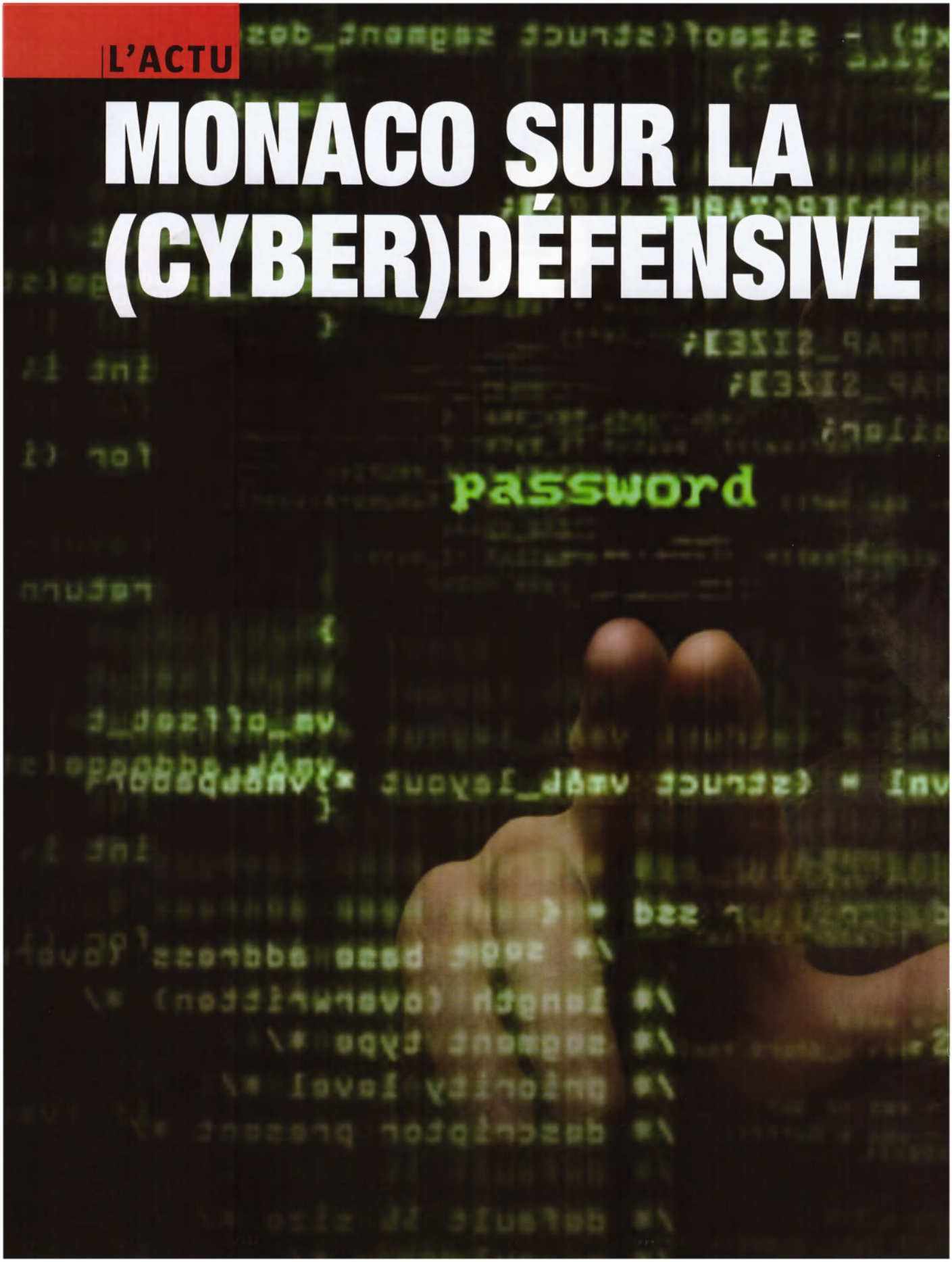
MONACO SUR LA (CYBER)DÉFENSIVE



Les infractions criminelles commises sur le web ne cessent de proliférer. Une plaie grandissante qui touche aussi bien les particuliers, les entreprises, que les structures publiques d'un Etat. Pour faire face à ces cyberattaques multiformes, le gouvernement monégasque a décidé de renforcer son arsenal législatif via « *un projet de loi de lutte contre la criminalité technologique.* » Déposé fin février 2015 au conseil national, ce texte — dense et relativement complexe — définit noir sur blanc l'ensemble des actes criminels numériques et prévoit des sanctions spécifiques.
Pour compléter ce cadre législatif, le gouvernement souhaite aussi mettre en place en 2015 une « *agence de sécurité numérique* », opérationnelle 24h/24 composée de 8 spécialistes. Cette structure de cyberdéfense monégasque aura pour rôle de prévenir les piratages en tout genre, et d'assurer la défense informatique des grands services et réseaux de l'Etat. Reste à savoir si les élus du conseil national voteront ou non ce texte et à quel point il sera amendé. Alors que les experts monégasques demandent un vote rapide, notamment en raison des engagements pris auprès du conseil de l'Europe, les parlementaires, eux, préferent prendre « *le temps de la réflexion.* » Histoire de mesurer, sans doute, si ces dispositions ne sont pas trop attentatoires aux libertés individuelles... _S.B.

SECURITE/ ESPIONNAGE INDUSTRIEL, USURPATION D'IDENTITÉ NUMÉRIQUE, ATTEINTES À L'E-RÉPUTATION OU ENCORE FRAUDES À LA CARTE BLEUE… LES INFRACTIONS COMMISES SUR INTERNET EXPLOSENT. JEAN-PHILIPPE NOAT ET BRUNO VALENTIN, EXPERTS INTERNATIONAUX EN CYBERCRIMINALITÉ ESTIMENT QU'IL EST URGENT QUE LA PRINCIPAUTÉ SE DOTE D'UN TEXTE LÉGISLATIF PROTECTEUR [1].

Cybercriminalité « Monaco peut subir de multiples attaques »

Monaco veut lutter contre la cybercriminalité avec un projet de loi qui devrait être prochainement voté. C'est un texte indispensable ?
C'est absolument primordial et j'espère qu'il sera voté très rapidement. Il faut bien se rendre compte de l'ampleur du phénomène. En 2013, au niveau mondial, la cybercriminalité a généré 323 milliards d'euros de pertes financières. En 2012, elle rapportait plus d'argent que le trafic de drogue (chiffres OCDE). Autre chiffre significatif : 7 millions de Français ont été victimes de cybercriminalité lors des 12 derniers mois. Soit 1 Français sur 8 (étude Symantec). Si l'on convertit ces chiffres à l'échelle monégasque, cela signifie que sur les 35000 habitants, plus de 4000 en ont été victimes. Il est donc urgent que chaque Etat puisse répondre pénalement à cette criminalité multiforme et la prévenir. Car Monaco, comme toutes les autres places, peut subir de multiples attaques de ce type.

De quels types d'infractions parle-t-on justement ?
La cybercriminalité recouvre les infractions pénales commises sur les réseaux numériques. Comme le piratage informatique, l'espionnage industriel, le défacement de sites web, les fraudes à la carte bancaire sur Internet, les décryptages de mots de passe, l'usurpation d'identité numérique, l'incitation à la haine ou encore les atteintes à l'e-réputation (réputation sur Internet)… Ce projet de loi monégasque permet de donner une véritable qualification à ces infractions numériques. Et donc une réponse pénale et des sanctions en conséquence.

« 7 millions de Français ont été victimes de cybercriminalité lors des 12 derniers mois. Soit 1 Français sur 8. »

Ce qui signifie que la cybercriminalité à Monaco est aujourd'hui impunie ?
Pas tout à fait. Car il y a des biais législatifs possibles pour sanctionner une infraction numérique. Par exemple, une fraude à la carte bancaire tombait sous le coup de l'escroquerie… Mais il est évident que ce texte donne une réponse moderne aux infractions de droit pénal classique.

Des exemples ?
Si une personne majeure ou une société est victime d'une atteinte à l'e-réputation à Monaco, c'est aujourd'hui compliqué de qualifier l'infraction et d'appliquer une sanction pénale. Car le préjudice en tant que tel n'est pas reconnu, ni clairement défini dans un texte de loi. Grâce à ce projet de loi, un résident victime d'une usurpation d'identité numérique sur Facebook, pourra dénoncer les faits. Autre exemple : l'intrusion dans un STAD (Système de traitement automatique des données) existait en France mais pas en principauté…

Qui sont les pirates informatiques ?
Il y a grosso modo trois types de pirates. Premièrement, les apprentis sorciers que l'on appelle les "script kiddies". Ce sont des néophytes qui regardent sur Internet comme on procède à un piratage… Ils se livrent alors au concours de celui qui pirate le plus de sites Internet. C'est un jeu. Deuxième type de pirates : ceux dont on ne parle pas. Il s'agit du pirate qui va être missionné par une entreprise concurrente pour faire de l'espionnage industriel. Ce sont ceux que l'on attrape pas ou peu. Il s'agit en général de professionnels. Il y a enfin de véritables réseaux mafieux.

AMENDEMENT/ «On peut durcir ce texte ou au contraire tomber dans l'angélisme», ont-ils dit Bruno Valentin et Jean-Philippe Noat (droite).

C'est-à-dire ?
Ils officient sur les parties moins visibles de l'Internet *(dark web)*, en vendant ou faisant usage des données piratées ou en proposant leurs services de hacking. Par exemple, sur le « dark web », il est possible de commanditer un déni de service pour bloquer complètement un site concurrent pour quelques centaines de dollars. Ceci en restant totalement anonyme. Il faut savoir aussi que des piratages entre pirates existent… Ils se livrent une guerre entre eux.

Le projet de loi prévoit la création à Monaco d'une autorité administrative spécialisée dans la lutte contre les cyber-menaces et cyber-attaques ? De quoi s'agit-il ?
C'est une sorte d'agence de sécurité numérique monégasque. L'équivalent en France est l'ANSSI (Agence nationale de la sécurité des systèmes d'information). Parmi ses missions, l'ANSSI est chargée de veiller à la protection des systèmes d'information du pays. Son rôle est d'anticiper et de réagir face à des incidents de sécurité qui touchent les infrastructures vitales de l'Etat. Comme les sites gouvernementaux ou plus généralement toute atteinte à un système d'information de l'Etat ou d'un OIV (Opérateur d'importance vitale).

« En 2013, au niveau mondial, la cybercriminalité a généré 323 milliards d'euros de pertes financières. En 2012, elle rapportait plus d'argent que le trafic de drogue. »

Des exemples concrets ?
Il peut s'agir d'une attaque d'un site gouvernemental ou visant un Etat dans son ensemble, comme l'Estonie il y a quelques années. Il peut s'agir aussi du piratage d'un système industriel qui provoquerait la prise de contrôle des

feux tricolores du pays par exemple… Ce type d'agence essaye d'anticiper le problème, et de détecter les vulnérabilités en amont de l'ensemble des acteurs.

Certains craignent que cette agence devienne une entité d'espionnage…
Ce projet de loi ne vise pas à espionner ni à surveiller les particuliers ou les entreprises. Au contraire, ce texte est là pour les aider et pour prévenir tout espionnage ou toute intrusion en provenance de l'étranger ou bien de la Principauté.

En quoi la création d'une agence de ce type à Monaco peut-elle permettre d'être plus efficace ?
Le projet de loi permet non seulement d'identifier et de prévenir les entités qui seraient piratées, mais aussi d'avoir une structure qui centralise toutes ces problématiques à l'échelle internationale et donc de bénéficier des retours d'expérience des entités équivalentes des différents pays. Ce qui n'existe pas aujourd'hui à Monaco. La coopération internationale est indispensable pour avoir une meilleure efficacité.

Quelles réticences pourraient provoquer ce projet de loi ?
Difficile à dire. Il faudra voir s'il sera amendé ou non. On peut durcir ce texte, ou au contraire… tomber dans l'angélisme. Monaco est aujourd'hui connue comme place forte de la sécurité des biens et des personnes. Elle pourra l'être bientôt comme place forte de la sécurité des données numériques. Ce qui pourra donc favoriser le développement de l'économie numérique.

On peut considérer qu'avec ce texte Monaco sera aussi bien protégé que la France ?
Je considère que ce texte, bien conçu, est en effet un très grand pas en avant. Monaco sera aussi bien protégé que la France, voire plus, car le projet de loi prend en compte les problématiques les plus récentes comme le stockage des données dans le Cloud ou le chiffrement des données.

Ce projet de loi va-t-il engorger les tribunaux et obliger les avocats à se spécialiser ?
La police monégasque s'est déjà adaptée. Les avocats et les magistrats seront en effet obligés de se spécialiser et de se familiariser avec cette matière, inévitable tant elle est transversale. En effet, à l'heure actuelle, les ordinateurs et les smartphones sont l'extension des individus et recèlent des informations intimes qui sont primordiales pour les procédures judiciaires.
La matière étant très spécifique, nous risquons d'assister à un phénomène similaire à celui qui est en train de se jouer dans les pays anglo-saxons.

« La police monégasque s'est déjà adaptée. Les avocats et les magistrats seront obligés de se spécialiser et de se familiariser avec cette matière. »

C'est-à-dire ?
Les cabinets d'avocats font maintenant appel à des cabinets de consultants spécialisés et disposant de ces certifications, pour mettre à mal les investigations techniques effectuées par les forces de l'ordre ou les experts, et fragiliser ainsi l'accusation. Des certifications de très haut niveau existent en la matière mais très peu de spécialistes les ont décrochées jusqu'à maintenant (3 en France et 2 à Monaco). Pour cette raison, nous avons suivi les mêmes cursus et décroché les mêmes certifications que ces consultants. Ceci afin d'apporter de la crédibilité et du poids aux expertises que nous effectuons. Nous incitons tous les experts que nous formons régulièrement au niveau européen à faire de même.

Selon une récente étude (étude Mandiant), 65 % des cyber-attaques ne seraient jamais détectées ?
En effet. C'est un chiffre énorme. La plupart des acteurs ne savent pas qu'ils sont piratés. Car ces piratages sont de plus en plus subtils et discrets.
En moyenne, une entreprise met 229 jours pour détecter qu'elle a fait l'objet d'une intrusion… C'est principalement là que le bât blesse. Une intrusion n'est en général pas détectée et les dossiers médiatiques comme le piratage de TV5 Monde (voir par ailleurs) sont l'exception puisque dans ce cas les attaquants voulaient avoir une visibilité. La situation est complètement différente quand les pirates désirent obtenir les données vitales d'une entreprise afin de lui extorquer de l'argent ou bien de valoriser les informations volées sur le « black market » (on parle souvent du dark web). Les pirates vont opérer par attaque ciblée et vont vouloir rester furtifs aussi longtemps que possible pour exfiltrer les données qu'ils convoitent (projets de recherche, liste des clients…).

A vous entendre, la cybercriminalité ne peut que s'aggraver ?
Jusqu'à présent, la cybercriminalité n'a fait, en effet, que s'aggraver. Il faut donc avoir le moins de retard possible et opérer une veille de tous les instants. Connaître les nouvelles formes de cybercriminalité, c'est connaître les nouvelles vulnérabilités. Pour se prémunir contre ces attaques informatiques, les sociétés peuvent faire auditer leur système d'information par des sociétés spécialisées pour faire détecter en amont les vulnérabilités qui le touche et faire ainsi estimer leur exposition face à ce type d'attaques.

Cela fait partie de vos missions ?
Nous intervenons régulièrement en effet auprès d'entreprises et d'institutions monégasques pour opérer, à leur demande, à des tests d'intrusion. Dans ce cas, nous pratiquons de la même façon que les pirates, avec la même méthodologie et les mêmes outils, et avec l'objectif d'obtenir nous aussi un accès au système d'information à l'insu de la société. Mais ce qui nous oppose aux pirates, c'est notre éthique. Nous pratiquons uniquement sur demande des entités, dans le but de les aider à renforcer leur défense.

ENJEU/ *« Très récemment, la société américaine Target en a été la victime. 110 millions de coordonnées bancaires (1 Américain sur trois) se sont dispersées dans la nature… »*

« En Estonie, l'Etat tout entier a été privé d'Internet pendant environ 2 semaines. Les distributeurs bancaires ne fonctionnaient plus. Le pays était paralysé. »

Le piratage peut générer de grosses pertes financières ?
Cela dépend du niveau de piratage. Si toute la base de données d'une société est piratée par exemple, les dommages sont considérables. Car toute la vie de l'entreprise est à l'extérieur. Très récemment, la société américaine Target en a été la victime. 110 millions de coordonnées bancaires (1 Américain sur trois) se sont dispersées dans la nature… L'entreprise a été condamnée à 10 millions de dollars à ses clients pour négligence. L'Estonie toute entière a également été victime d'un DDOS (attaque par déni de service)

De quoi s'agit-il ?
Un DDOS bloque la totalité des infrastructures d'une société, d'un gouvernement ou d'un Etat. En Estonie par exemple, l'Etat tout entier a été privé d'Internet pendant environ 2 semaines. Les distributeurs bancaires ne fonctionnaient plus. Le pays était paralysé.

_SABRINA BONARRIGO.

(1) Bruno Valentin et Jean-Philippe Noat sont aussi experts judiciaires en investigation numérique en France et à Monaco et formateurs internationaux en cybersécurité et cybercriminalité.

SOCIÉTÉ/

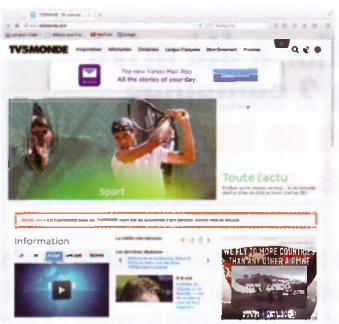
Anonymous et le djhad : une traque « totalement contre-productive »

Anonymous a déclaré la guerre aux djihadistes sur Internet... Après les attentats à *Charlie Hebdo*, ce groupe de hackers internationaux s'est lancé une mission : traquer les sites web faisant l'apologie du djihad. Ils l'ont fait savoir via une vidéo au message on ne peut plus limpide : *« La liberté d'expression a été meurtrie. Attaquer la liberté d'expression, c'est attaquer Anonymous. Nous ne le permettons pas. Toutes entreprises en lien avec ces attaques terroristes doivent s'attendre à une réaction massive d'Anonymous. Nous vous traquons. »* Ces "justiciers du web" ont notamment publié dans la foulée une liste de 120 comptes Twitter désignés comme *« islamistes »*, puis une liste de 89 comptes Twitter dits *« terroristes »*. Pourtant, pour les experts monégasques, on est bien loin d'un acte *de* "hackers citoyens". Ils estiment au contraire qu'il s'agit là d'un message *« totalement contre-productif. »* La cause ? Ces hackers parasiteraient — voir anéantiraient — le travail des enquêteurs spécialisés. *« Depuis longtemps, il existe une veille sur le cyberterrorisme. Un travail de très grande ampleur est accompli par les services spécialisés pour identifier les comptes terroristes sur les réseaux sociaux*, expliquent Jean-Philippe Noat et Bruno Valentin. *En communiquant publiquement ce message, les Anonymous ont mis à terre tout ce travail de prévention et de veille car les terroristes vont bien sûr changer de compte et d'environnement. De ce fait, l'avance qu'avaient les forces de l'ordre s'en trouve diminuée. »* _S.B.

ATTAQUE/

Ecran noir sur TV5 monde

C'est une attaque d'une ampleur inédite qui a visé la chaîne TV5 Monde. Le mercredi 8 avril vers 22 heures, des pirates se réclamant du groupe djihadiste Etat islamique ont paralysé l'ensemble du système informatique de la chaîne. Pendant plusieurs heures, c'est donc un écran noir qui a remplacé les programmes habituels. Même les comptes Facebook, Twitter et le site internet, ont été piratés. Sur ces sites, on pouvait lire le titre *« Cybercaliphate »* et *« Je suIS IS »* (ISIS est l'acronyme anglais qui désigne l'Etat islamique), un détournement du slogan *« Je suis Charlie »*. Ce n'est que le lendemain que la chaîne a rétabli progressivement ses programmes.



« Il semblerait que l'attaque ait tout d'abord été furtive par la prise de contrôle du site internet et des réseaux sociaux (Facebook, twitter). Cette prise de contrôle n'est en général pas détectée ou détectée très tardivement, sauf si des signes extérieurs apparaissent comme un changement de la page d'accueil. En simultané, il a suffi de faire tomber le réseau informatique de TV5 par un DDOS ciblé (donc une attaque paralysant le réseau) et de prendre le contrôle du site », expliquent Jean-Philippe Noat et Bruno Valentin. Pour ces deux experts en cybercriminalité, une des causes de cette attaque peut être un manque d'anticipation mais aussi l'utilisation de mots de passe trop simples ou identiques sur tous les réseaux sociaux : *« Seule l'anticipation permet de faire face à ce genre d'attaque en auditant régulièrement son système d'information et en simulant ce genre d'attaque. »* _S.B.

Monaco sous contrôle 24h/24 ?

CYBERDÉFENSE/ Une agence de sécurité numérique, opérationnelle 7 jours sur 7, devrait être créée à Monaco dans le courant de l'année 2015. Son rôle sera notamment de prévenir, détecter et traiter toute cyberattaque.

Monaco a décidé de mettre les bouchées doubles en matière de cybercriminalité. Au-delà d'un nouvel arsenal législatif[1], une agence de sécurité numérique active 24h/24 et 7 jours sur 7, devrait voir le jour dans le courant de l'année 2015. Cet organisme — dépendant directement du département de l'Intérieur — serait composé à moyen terme de huit personnes. Une mini "cyberarmée" de spécialistes pour se prémunir des *« nombreuses menaces »* dont regorge la Toile. *« Les attaques peuvent prendre différentes formes : détruire, altérer ou encore accéder à des données sensibles dans le but de les modifier ou de nuire au bon fonctionnement des réseaux et des personnes publiques et privées,* explique le département de l'Intérieur. *Au-delà des coûts annuels s'élevant à des milliards d'euros que des fraudes numériques génèrent dans le monde, en particulier, pour les banques et les entreprises, il convient de relever que les systèmes d'information peuvent offrir des services vitaux ou essentiels sur lesquels reposent la sûreté et l'économie nationales des Etats. »* Pour le gouvernement donc pas de doute : la sécurité numérique est devenue *« un véritable enjeu de souveraineté. »*

Cet organisme dépendant du département de l'Intérieur serait composé de huit personnes.

Sensibiliser

Quelles seront alors les missions de ces « pompiers du web « monégasques ? Le gouvernement a dévoilé à *L'Obs* les grandes lignes : prévenir, détecter et traiter les cyberattaques *« notamment par l'élaboration de plans, de procédures, de dispositifs de protection et de précaution »* ; réagir en situation de crises provoquées par des cyberattaques, mais aussi sensibiliser les services publics et les opérateurs d'importance vitale (OIV) aux exigences de la sécurité numérique. *« Son rôle sera également de contrôler le niveau de sécurité des opérateurs de communications électroniques (exploitant de réseau ou fournisseur de services de télécommunications ou d'accès à Internet), en concertation avec la direction des communications électroniques »*, détaille le département de l'Intérieur.

Coûts

Côté budget, une première enveloppe de 1,5 million d'euros a déjà été débloquée. Une somme conséquente car outre le recrutement de spécialistes très pointus, cette agence nécessite un aménagement spécifique de locaux et l'acquisition de matériels de très haute performance. *« Ceci explique le conséquent budget initial dédié à la création de cette agence. Son coût annuel de fonctionnement devrait être en revanche plus modeste et se résumera essentiellement au coût salarial de cette structure »*, précise encore le gouvernement.

_SABRINA BONARRIGO

(1) Cette agence est l'une des mesures phares prévue dans projet de loi sur la criminalité technologique déposé fin février 2015 sur le bureau du conseil national (article 22).

Les cyberattaques en chiffres

Année	2013	2014
Infractions[1] commises sur Internet dont :	108	51
• usages frauduleux de coordonnées bancaires (UFCB)	89	31
• escroqueries sur Internet (autres que UFCB)	16	14
• piratages informatiques (usurpations d'identité, d'adresse mail, etc.)	3	6

(1) Infractions ayant fait l'objet d'une déclaration à la direction de la Sûreté publique.