REVUE DE POLICE

Décembre 2021 - N° **42**

Publiée par la Direction Générale de la Sûreté Nationale

LA CYBER SECURITE

POUR UN CYBERESPACE PLUS SÛR

La Brigade cynotechnique ..

Composante importante du dispostif de sécurité mis en place à l'occasion de la fin de l'année 2021

LA CYBER SECURITE

nouvelle génération des défis sécuritaires

La société et notre mode de vie, se sont littéralement transformés avec l'avènement des nouvelles technologies de l'information et de la communication et la démocratisation d'Internet. La société entière se digitalise. Le cyberespace, ce nouvel espace virtuel, est devenu alors l'arène de vie, de services, de travail, d'enseignement, d'expression, de divertissement, de positionnement, etc. Un univers dématérialisé où les frontières sont abolies et les systèmes fortement interconnectés.

Mais si le numérique offre tant d'opportunités de développement économique, de souveraineté et de bonne gouvernance, il est aussi porteur de risques et de menaces. Le risque « cyber » vient alors, s'ajouter aux autres risques à prendre en considération, au même titre que le risque financier, technologique ou autre. Se prémunir contre le cyber-risque devient alors un enjeu stratégique.

La cybersécurité est devenue de fait, une spécialité sécuritaire à part entière, indispensable et incontournable, pour un cyberespace plus sûr.

En effet, dans ce monde virtuel connecté, de nombreuses vulnérabilités sont apparues dans les réseaux et les systèmes d'information, qui à leur tour ont donné lieu à de nouvelles menaces, en constante évolution, souvent plus complexes et plus graves que les menaces traditionnelles et les risques classiques.

Ces vulnérabilités ne sont en fait, qu'une conséquence logique et inévitable de la spécificité du «cyberespace », constitué par l'imbrication et l'interaction d'un ensemble de réseaux et de systèmes, ce qui le rend unique et radicalement différent du monde physique, car c'est un espace sans frontières connues, en constante évolution et transformation, dans lequel il est difficile d'identifier, d'anticiper ou de prévoir les formes de criminalité qui peuvent s'y produire.

> **Si le numérique offre tant d'opportunités de développement économique, de souveraineté et de bonne gouvernance, il est aussi porteur de risques et de menaces**

Dans cet espace virtuel, la criminalité avec ses diverses déclinaisons et catégories y a trouvé sa place, s'est adaptée et s'est numérisée. Une menace protéiforme et diversifiée, que ce soit au niveau des techniques et des méthodes utilisées, qu'au niveau des cibles, ou même des auteurs présumés, profitant amplement du développement rapide et des potentialités offertes par le numérique (anonymat, dark web, instantanéité, etc).

En termes de répercussions et d'impact, personne ne peut nier qu'une simple cyberattaque pourrait mettre gravement en danger la survie d'une organisation particulière, les intérêts de tout un pays ou lui causer de grands dommages, et pourrait même, dans de nombreux cas, nuire gravement à son image et sa notoriété. Le récent dysfonctionnement des réseaux sociaux survenu le 08 octobre 2021 en est l'illustration magistrale, où une panne temporaire des serveurs du géant d'Internet «META» (anciennement Facebook) a entraîné la coupure de la communication virtuelle dans tous les pays du monde, et a remis sur la table les discussions sur le problème que représentent les médias sociaux comme seul canal pour connecter le monde.

Qui sont alors les cibles potentielles ? La réponse est simple: Tout le monde!
Individus, Institutions, entreprises... Les cyberattaques peuvent viser des individus dans le but d'accéder frauduleusement à leurs données personnelles pour les utiliser à des fins illégales, comme les entreprises et les institutions publiques, sous forme d'intrusions dans leurs systèmes d'information et pouvant atteindre des niveaux stratégiques au sein d'un Etat, en ciblant les systèmes de défense nationale, de sécurité nationale et des intérêts économiques.

Quant aux modes opératoires et moyens techniques utilisés aux fins de perpétrer ces cyberattaques, ils diffèrent selon la nature et le niveau des cibles visées. Les attaques peuvent aller d'une simple intrusion via des malwares «open source» sans aucun coût, à une série d'autres, plus sophistiquées utilisant des programmes complexes et coûteux, visant à paralyser complètement le système d'information d'une infrastructure vitale ou stratégique.

Dans ce monde virtuel où pullulent ces menaces de tous genres, la cybersécurité est devenue une composante essentielle et un enjeu de sécurité nationale, à prendre en compte à tous les échelons, pour faire face à l'évolution fulgurante des cybermenaces, qui gagnent chaque jour du terrain et ne cessent de progresser, afin de garantir un cyberespace plus sûr et plus sécurisé et protéger ainsi notre société numérique.

La cybersécurité est plus que jamais, placée au centre des préoccupations des pays du monde entier, qui cherchent à mettre en place des stratégies intégrées de prévention, de détection et de réponse aux cyberattaques, et à développer des solutions technologiques à la hauteur des défis de la menace « cyber » qui guette tout le monde

La Revue de Police a consacré ce nouveau numéro à la cybersécurité et aux efforts louables déployés au niveau national, pour un cyberespace plus sûr et une plus grande confiance, pour une transformation numérique à pas sûrs, favorisant le développement de notre société, tel que voulu par le nouveau modèle de développement, initié par ***Sa Majesté le Roi Mohammed VI, que Dieu L'assiste*** ■

Rédacteur en chef
Boubker Sabik

Responsable administrative
Amal BERKIA

Responsable artistique
Hamid CHAFI

Photos
- Saad CHERRADI
- MAP

Rédaction
-Boubker Sabik
- Amal BERKIA

Dessins
- Issam EL ASRI
- Khalid EDDAOUDI

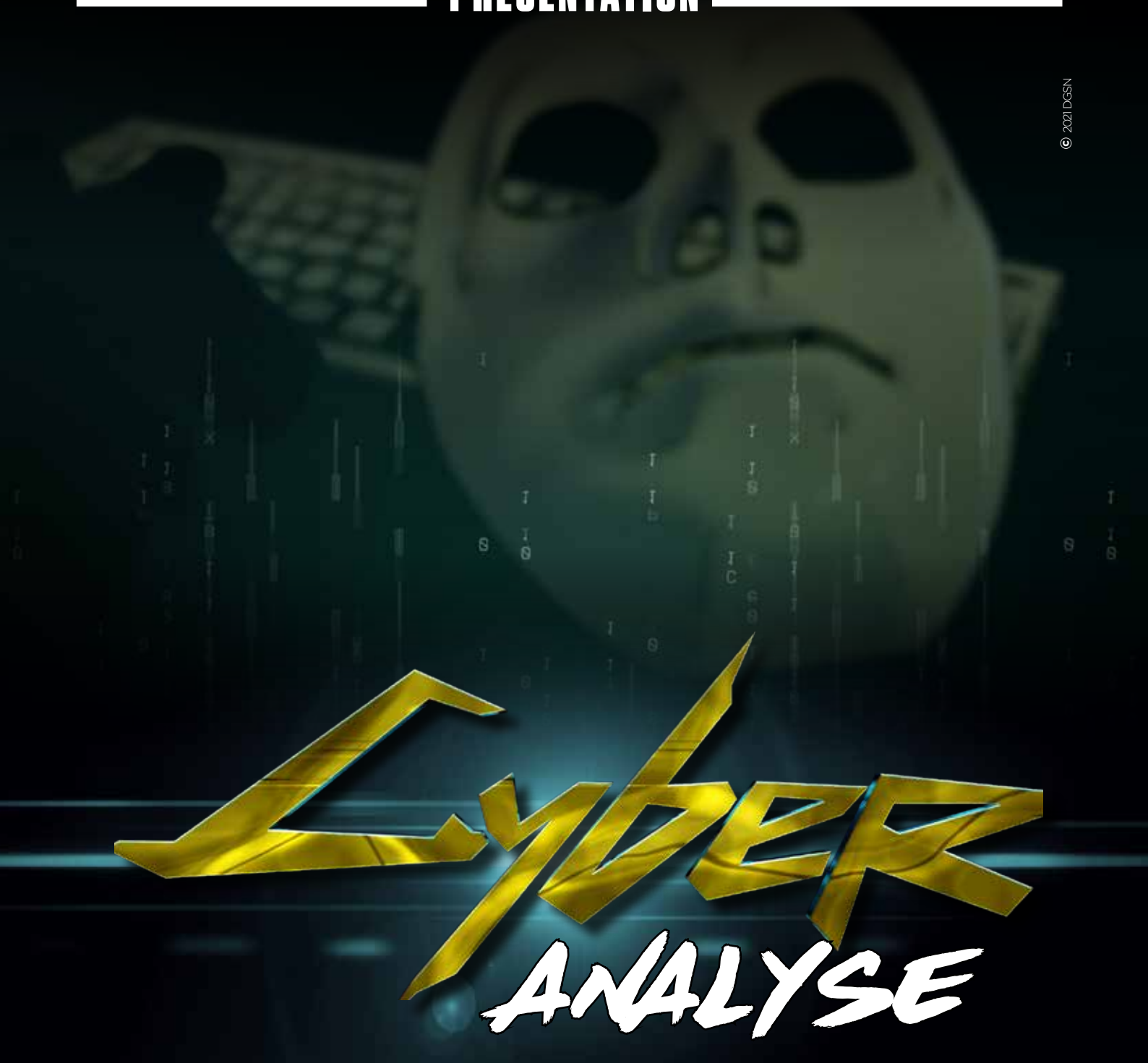
Tirage
2.000 exemplaires

Impression
Imprimerie R-PRINT

Dépôt légal : 2005/0010
ISSN : 1114-8349

Adresse
Revue de Police
N°3 Rue Chrarda,
quartier administratif
Takadoum - Rabat. BP 437

Téléphone 0537636707
Fax 0537651503
Email
revuedepolice@dgsn.gov.ma



De nos jours, notre vie ressemble de plus en plus à une *cybervie*. En effet, on a l'impression de naviguer dans un cyberespace, sans penser aux risques éventuels, qu'on soit sur son 31 ou dans son pyjama et ses pantoufles, on a l'impression de se balader tranquillement, ne se doutant de rien, ne se souciant de rien, pensant que rien ne peut nous atteindre. Pourtant, jeune ou vieux, expert ou pas, le danger nous guette à chaque clic sur un lien (hyperlien), le cyber danger !!

Si au début des années 90, on parlait de virus qui pouvaient se propager sur quelques ordinateurs d'un réseau local, aujourd'hui, et avec le développement et la croissance fulgurante d'Internet et la sophistication des modes d'attaques, on arrive facilement à plusieurs millions d'ordinateurs, qui peuvent être infectés rapidement par un virus informatique ou un malware. Des virus ou malwares qui se propagent dans vos machines via des e-mails, sur le Web, les terminaux mobiles ou les applications informatiques, pour voler vos données, votre identité, ou encore rendre votre système indisponible ou pire encore, chiffrer vos données pour vous demander une rançon, ou faire usage de votre machine, à votre insu pour générer de la cryptomonnaie. ***WannaCry*** n'est certainement pas le seul code malvaillant qui a infecté des centaines de milliers d'ordinateurs dans plus de 150 pays, et dont le préjudice a été évaluée à plusieurs centaines de millions de Dollars US. Les activités de rançongiciels auraient généré en 2020, plus de 350 millions Dollars US (d'après Chainalysis). Le panorama des cyberattaques et des cyberescroqueries ne cesse de s'élargir et se perfectionner.

Pour leur part, les criminels du Web, ces opportunistes, dont l'expertise ne cesse malheusement de croître, profitent de ces technologies pour en tirer illégalement des bénéfices. Ces cybercriminels, au début d'Internet, communément appelés Hackers ou black hat, leur profil était davantage, celui de jeunes adolescents en mal de reconnaissance, voulant s'amuser et se faire remarquer. De nos jours, ce sont de vrais professionnels, en quête d'argent et de grandes arnaques. Chaque personne qui se connecte maintenant sans se protéger « logiquement » est une cible parfaite pour ce genre de criminels, surtout avec la croissance rapide des services « online », banque en ligne, inscription en ligne, réservations en ligne, shopping en ligne, etc. Le danger est malheureusement partout !!!

Ces opportunistes profitent également de chaque crise pour orchestrer leurs attaques. L'exemple concret, est la crise pandémique de la COVID-19. Des applications mobiles diverses sur la situation pandémique ont fleuri, et qui ne sont autres que des *maliciels* déguisés pour mettre la main sur vos données et vos machines.

Un autre volet très important, ce sont nos données personnelles. Nombreuses sont les personnes qui mettent leurs données personnelles, pour ne pas dire, leur vie quotidienne sur les réseaux sociaux, sans penser un instant qu'elles pourraient être exploitées par un escroc.

Dans le monde virtuel, maintenant, on peut trouver tout ce qui peut exister dans le monde du business « réel », fabricants, détaillants, fournisseurs, clients, etc.

Pour plusieurs personnes, se faire de l'argent dans ce monde parallèle est le terrain de prédilection pour le crime organisé, sans aucun contrat physique avec les partenaires d'affaires. L'économie souterraine de ce monde, offre une variété de produits et de services et où les criminels trouvent leur «bonheur», en créant des comptes avec des identités usurpées et assez complets, se faufilant à travers une sécurité quasi inexistante, sans le moindre remord, ne connaissant même pas leurs victimes, du moins physiquement.

Récemment, on entend parler de cyberguerre, alors qu'il n'y a pas de victimes humaines, mais qui peut paralyser un pays, ou causer des pertes financières importantes pouvant ruiner tout un pays et réduire à plat son économie

Récemment, on entend parler de cyberguerre, alors qu'il n'y a pas de victimes humaines, mais qui peut paralyser un pays, ou causer des pertes financières importantes pouvant ruiner tout un pays et réduire à plat son économie. Mais s'il s'agit de systèmes vitaux, tels que les centrales électriques ou d'eau potable, je vous laisse imaginer les dégâts indirects que cela peut causer, en injectant un virus ou un malware dans de tels systèmes.

Il est clair que si Internet a apporté beaucoup de services bénéfiques et rapides, il a aussi apporté

avec lui, son lot de dangers et d'autres problèmes qu'il faudrait pouvoir résoudre virtuellement.

La sécurité du cyberespace.. une prise de conscience globale et intégrée

La Société en tant qu'entité intégrée et globale, avec son économie, ses citoyens, son business, ses infrastructures, ses administrations, son gouvernement, etc., sont exposés aux cyberattaques qui peuvent handicaper leur fonctionnement. Il est de ce fait clair que pour y faire face, les gouvernements sont amenés à développer des actions globales et intégrées, tant sur le plan juridique, organisationnel et technique, que sur le plan du partenariat public-privé et de la coopération internationale, avec plusieurs acteurs et dans un cadre totalement légal, technique, public et privé, national et international.

Cybersécurité et protection des données personnelles sont des aspects qui peuvent quelques fois être antagonistes ou contradictoires, surtout pour les services de sécurité qui essaient dans certains cas de collecter des informations sur certains individus suspects, mais en réalité, il y a plutôt une certaine synergie entre les deux, puisqu'un haut niveau de cybersécurité va privilégier une meilleure protection des données personnelles. Les nouvelles technologies et Internet ont transformé notre façon de communiquer, d'accéder à l'information, de discuter dans un groupe, faire nos achats, etc., et bien sûr, la manière de perpétrer un crime. Comme la technologie avance à pas de géant, les criminels l'utilisent aussi pour perpétrer leurs actes presque en toute impunité, d'où une activité de cybercriminalité assez croissante et le bien le plus précieux qu'ils recherchent est la «DATA », vous dépouiller ainsi de votre droit à la confidentialité privée, d'autant plus qu'il est plus ou moins aisé de rester anonyme sur le cyberespace, que les frontières n'existent pas et que les législations diffèrent d'un pays à l'autre, ce qui rend les poursuites judiciaires plus ardues.

La DGSN, a néanmoins, pris le devant depuis plusieurs années déjà, pour sensibiliser les jeunes sur les méfaits d'Internet durant les campagnes de sensibilisation en milieu scolaire qu'elle effectue dans les écoles, collèges et lycées.

En 2021, on a prédit qu'il y aurait une cyberattaque dans le monde toutes les 11 secondes, ce qui, comparé à 2016 (40 secondes) est quatre fois plus grand. La cybercriminalité cause des dommages qui sont estimés à près de 06 Trillions de Dollars US annuellement en 2021, et va sans nul doute certainement croître jusqu'à plus de 265 Trillions de Dollars US en 2031 (d'après cybersecurity Accenture).

Des chiffres qui font froid au dos et qui reflètent bien les futurs défis qui attendent les services de sécurité et qu'il convient de s'y préparer convenablement et rapidement. Le coût englobe, dommages et destruction des données, argent volé, perte de productivité, fraudes, réputation, etc. Concernant le Darknet (réseau Internet non indexé), on estime qu'il serait 5.000 fois plus important que sur la toile Internet classique, et qu'il croît à un rythme effréné.

Au Maroc, la prise de conscience de l'importance de la cybersécurité a été matérialisée par la mise en œuvre de deux textes fondateurs, la loi sur la cybersécurité et celle sur les services de confiance, ainsi que la création d'organes de gouvernance, notamment l'autorité nationale de la cybersécurité, qui n'est autre que la Direction Générale de la Sécurité des Systèmes d'Information relevant de l'Administration de la Défense Nationale. En matière de lutte contre la cybercriminalité, composante essentielle de toute stratégie de cybersécurité, la DGSN s'est dotée de cybercapacités en termes d'investigations sur la toile et de digital forensic, pour traquer les criminels sur la toile et apporter la cyberpreuve tangible, afin de les traduire en justice.

La cybesécurité..une culture à instaurer

Les internautes passent en moyenne 7 heures sur Internet (d'après We are social et Hootsuite) et les jeunes d'aujourd'hui ne peuvent plus se passer d'Internet dans leurs activités quotidiennes et l'utilisent tout le temps, même à des heures très tardives de la nuit, pour ne pas dire la nuit entière. D'un autre côté, ils sont les plus vulnérables à communiquer leurs données personnelles, à l'endoctrinement, facilement influençables, pas forcément conscients des dangers qui les guettent dans la toile, et demeurent des proies faciles pour les cybercriminels, plus que les adultes. D'un autre côté, ces jeunes ne dénoncent pas toujours ces crimes aux forces de sécurité, ce qui rend difficile la lutte et la prévention contre cette forme de criminalité. La DGSN, a néanmoins, pris le devant depuis plusieurs années déjà, pour sensibiliser

les jeunes sur les méfaits d'Internet durant les campagnes de sensibilisation en milieu scolaire qu'elle effectue dans les écoles, collèges et lycées. Aussi, une nouvelle plateforme nationale baptisée «e-Himaya», a été lancée en décembre 2021 par l'Agence de Développement du Digital, en coordination avec les parties prenantes, dont la DGSN, dédiée à la protection des enfants en ligne. Ceci n'empêche pas que les parents doivent jouer un rôle plus important dans la surveillance de leurs progénitures dans les réseaux sociaux, et s'approcher davantage de leurs enfants pour détecter et signaler tout comportement suspect.

La cybercriminalité..des modes opératoires de plus en plus sophistiqués

Difficile d'imaginer un monde sans Internet, il a transformé notre planète en un petit village virtuel sans frontières. Les nouvelles technologies ont complètement métamorphosé notre façon de communiquer, d'exprimer nos idées, de protester, de chercher et trouver l'information, et par conséquent, la naissance d'un autre terrain propice au crime, un cyberespace qui ne cesse de croître et d'intégrer une multitude de services et donc, d'occasions de perpétrer des crimes dans l'anonymat total et en ciblant une masse importante de victimes, en un temps record. Les menaces se diversifient, deviennent de plus en plus complexes et n'épargnent personne, les individus, les institutions et les entreprises.

La majorité des cybercrimes peuvent être résumés en gains financiers, espionnage ou cyberespionnage, endoctrinement idéologique, harcèlement, etc., mais les crimes à but purement lucratif demeurent les plus prédominants. En outre, avec le web sémantique et l'avènement des réseaux sociaux, Internet est devenue l'arène d'expression par excellence, où la désinformation y a trouvé sa place, conjuguée au deepfake, ayant recours à l'intelligence artificielle, pour truquer les images et la voix, où tout devient possible et accessible.

Et si le panorama des cybercrimes s'élargit de jour en jour, phishing, rançongiciels, minage, business mail compromise, vol de données personnelles, usurpation d'identité, etc., le danger réel du futur cybercrime réside dans le darkweb ou deepweb, cette partie invisible du Net qui dépasse largement le web indexé en surface (Internet classique) et croît de manière exponentielle, et qui contient des informations invisibles pour le web surfacique, avec des activités illégales, telles que la pédopornographie, le blanchiment d'argent, le vol d'identités, le marché noir des armes, des drogues, pour ne citer que celles-ci. Ce darkweb qui utilise le cryptage à outrance et masque les adresses IP, ce qui les rend difficiles à identifier. Pire encore, les cybercriminels s'organisent, recrutent de nouveaux membres et mettent en vente leur « savoir», la cybercriminalité « as a service ».

En dépit de l'émergence de ces menaces qui sont bien réelles, un espoir est porté sur le deep Learning et l'intelligence artificielle, pour améliorer la cybersécurité dans le cyberespace, qui peut détecter très tôt des comportements anormaux plus vite que l'être humain, constituant ainsi, un outil précieux pour les cyber-policiers pour anticiper les cyberattaques ■

© 2021 DGSN

LA DGSSI..

Rempart Contre les cyberattaques et garant de la cybersécurité des systèmes d'information vitaux de notre pays.

Par
le Général de Brigade EL Mostafa RABII

Directeur du Centre de veille, de détection et de réponse aux attaques informatiques **m@CERT**, à la DGSSI

D epuis 2012, le Maroc a adopté une approche transversale en matière de cybersécurité, tant au niveau réglementaire qu'institutionnel. C'est ainsi qu'une Agence Nationale de la Sécurité des Systèmes d'Information a vu le jour et à laquelle a été confiée la mission de mise en œuvre de la stratégie nationale régissant ce domaine. Cette Agence, n'est autre que la Direction Générale de la Sécurité des Systèmes d'Information «DGSSI», relevant de l'Administration de la Défense Nationale. Un vivier de compétences de pointe, tant dans le domaine technique que juridique, travaillant de jour comme de nuit, traquant tout incident aussi faible soit-il, pouvant compromettre les infrastructures vitales de notre pays.

© 2021 DGSN

La cybersécurité.. des enjeux et des stratégies

Le développement du digital se place aujourd'hui au cœur des enjeux socio-économiques et de défense des pays. L'importance du numérique dans les échanges, les services, les transactions ne fait qu'augmenter avec les besoins croissants de consolidation des données, d'accès aux données en temps réel depuis n'importe quel point de la planète, et de réduction des coûts. De surcroît, la convergence des domaines des Télécoms et de l'informatique d'une part, et la convivialité d'adoption du Cloud et de l'Internet des objets (IoT), d'autre part, ont précipité davantage cette digitalisation, particulièrement aux niveaux des institutions de l'Etat et des entreprises.

Par ailleurs et au vu des avantages que procurent les systèmes numériques de contrôle industriel et les logiciels de supervision et de contrôle (SCADA), les secteurs de l'énergie électrique, du pétrole et du gaz, de la fabrication, de l'eau, des transports, des produits chimiques, etc. recourent désormais à outrance à ces systèmes d'information industriels, qui sont souvent connectés aux réseaux de gestion et parfois directement à Internet. Cette tendance s'accentuera de plus en plus avec la démocratisation du Big-data et de l'intelligence artificielle.

Certes, cette transition numérique est porteuse d'innovation et de croissance, mais crée aussi une immense surface d'attaque qui profite forcément aux cybercriminels. Cette surface s'est vue agrandir davantage avec la migration massive vers le télétravail dans les secteurs public et privé, suite aux restrictions imposées par la pandémie de la Covid-19. Ainsi, les vulnérabilités matérielles, logicielles et de configuration non corrigées d'une part, et l'absence de solutions de sécurité, d'autre part, sont à chaque instant exploitées et mises à profit pour mener des cyberattaques.

La menace «cyber»..diffuse, discrète, mais bien réelle.

L'étendue du cyberespace, son ouverture et sa perméabilité vis-à-vis de l'international en font une source de vulnérabilité. En même temps, la facilité d'accès au savoir-faire et aux outils nécessaires au piratage informatique font que chaque jour de nouvelles vulnérabilités critiques sont détectées et de nouveaux vecteurs d'attaques sont développés et partagés sur le Net. Ainsi, au fil des années, les cyberattaques se sont multipliées et diversifiées et ont augmenté proportionnellement avec l'évolution de la surface d'attaque.

La cybermenace est diffuse, souvent discrète, mais bien réelle comme l'illustre la série de cyberattaques très médiatisées qu'a connues l'année 2021, notamment celles ayant trait à Microsoft Exchange, SolarWinds ou Colonial Pipeline. A titre d'exemple, une vague mondiale de cyberattaques et de violations de données a été enregistrée suite à la découverte de plusieurs exploits de type «zero-day» dans des serveurs de messagerie Microsoft Exchange. Microsoft a certes publié des mises à jour afin de corriger les failles, mais cela n'a pas permis d'éviter les dommages enregistrés ou de supprimer les portes dérobées installées par les attaquants. Par la suite, une nouvelle famille de ransomwares a été déployée sur les serveurs initialement infectés, chiffrant tous les fichiers, rendant le serveur inopérant et exigeant un paiement pour réparer les dommages. Cet exemple montre que ***personne n'est à l'abri d'une cyberattaque, pas même les grandes sociétés informatiques.***

Toujours dans le sillage des attaques informatiques, le nombre de violations de données, en 2021, a dépassé de manière significative celui de 2020, selon l'Identity Theft Resource Center (ITRC). De même, un rapport d'Accenture a révélé que le volume des cyber-intrusions dans le monde a enregistré un bond de 125% au premier semestre 2021 par rapport à la même période de l'année précédente. Quant aux attaques de ransomwares, ils ont enregistré une augmentation de 62 % depuis 2019, selon le rapport sur les cybermenaces 2021 de SonicWall.

*Le nouveau modèle de développement, dont les contours et les principes ont été définis par **Sa Majesté le ROI, que Dieu L'assiste,** a retenu le numérique comme un axe transverse pour la réforme de l'administration, ainsi que le développement économique et social de notre pays*

La cybersécurité..la réponse aux menaces

En quête d'une posture de cybersécurité efficace, les pays tentent aujourd'hui de réglementer le cyberespace. Mais, le fait qu'Internet soit considéré comme un espace de liberté absolu pour certains pays et un espace qui doit être supervisé pour d'autres, rend difficile l'atteinte de cet objectif, qui nécessite de facto une collaboration internationale intense. Pire encore, plusieurs pays considèrent cet espace comme un nouveau champ de bataille. Devenu un espace de conflictualité, la tâche des responsables de la cybersécurité s'est compliquée davantage, notamment en ce qui concerne la protection des infrastructures d'importance vitale.

Dans ce contexte international mitigé, chaque pays doit se doter de capacités pour prévenir les cybermenaces, pour assurer la disponibilité, la confidentialité et l'intégrité des systèmes d'information et pour réagir promptement aux cyberattaques. A cet égard, le développement d'une forte culture de cybersécurité et le renforcement de la résilience des systèmes d'information sensibles sont des prérequis essentiels.

Le Maroc et suite aux **Hautes Directives de SM le ROI, que Dieu L'assiste**, a très tôt pressenti la nécessité d'une réponse aux enjeux que présentent la cybersécurité. Cette prise de conscience a permis, dès 2011, de doter le pays d'instances adéquates de gouvernance de la cybersécurité, de capacités de supervision et de moyens de réaction nécessaires, ainsi que d'une règlementation conforme aux standards internationaux. Ces mesures ont permis d'accroître la confiance dans l'environnement numérique national, de protéger les organismes de l'Etat et les infrastructures d'importance vitale contre les cybermenaces, et de mettre en place un cadre de collaboration entre l'Etat, le secteur privé et les universités dans ce domaine très pointu et complexe.

Enfin, le nouveau modèle de développement, dont les contours et les principes ont été définis par **Sa Majesté le ROI, que Dieu L'assiste**, a retenu le numérique comme un axe transverse pour la réforme de l'administration, ainsi que le développement économique et social de notre pays. Le recours massif, à cet effet, à la dématérialisation contribuera certainement, par ricochet, à un développement rapide de l'écosystème de cybersécurité national. Ce qui appuiera pleinement les efforts déployés par les acteurs en charge de la lutte contre la cybercriminalité, la protection des données personnelles et la cyberdéfense, et partant, la promotion d'un espace de confiance numérique de haut niveau.

© 2021 DGSN

Le m@CERT..

BRAS OPÉRATIONNEL DE LA DGSSI

Partie intégrante et bras opérationnel de la Direction Générale de la Sécurité des Systèmes d'Information, le centre marocain de veille, de détection et de réaction aux attaques informatiques (maCERT : Moroccan Center of Emergency Response Team), est une composante fondamentale du dispositif national de lutte et de protection contre les attaques cybernétiques

© 2021 DGSN

Le m@CERT..rempart contre les menaces cybernétiques

A l'instar des pays avancés sur le plan de la cybersécurité, le Maroc, soucieux de faire de la transformation digitale maîtrisée et sécurisée, un levier de son développement économique et social, s'est donné les moyens humains et techniques pour doter la DGSSI d'une structure permettant d'assurer à la fois des actions actives et proactives, à même d'appréhender la menace cybernétique à travers notamment, une veille sur les évolutions technologiques, ainsi que sur les vulnérabilités qui en découlent. A travers une supervision et une évaluation continues des systèmes d'information nationaux et connaissant le panorama des risques qui les guettent, le maCERT est en mesure de proposer des recommandations techniques et organisationnelles susceptibles de renforcer la protection et la résilience des SI de notre pays. Pour assurer ses missions, le maCERT dispose de cadres formés dans différents domaines de la cybersécurité, tels que: l'analyse des malwares, les tests d'intrusion, la veille et la supervision et la réaction aux cyberattaques.

> *Le m@CERT est en mesure de proposer des recommandations techniques et organisationnelles susceptibles de renforcer la protection et la résilience des SI de notre pays.*

Le m@CERT face à la pandémie de la Covid-19

Face à la pandémie de la Covid-19, le maCERT a mobilisé ses ressources pour lutter contre l'augmentation significative du nombre de campagnes de phishing, d'attaques de ransomwares et d'ingénierie sociale liées à cette crise sanitaire. Un soutien particulier a été aussi apporté aux administrations, organismes publics et infrastructures d'importance vitale pour sécuriser le télétravail et accompagner la dynamique générée par les projets de digitalisation mis en place pour répondre aux défis imposés par cette pandémie.

Le m@CERT..rempart contre les menaces cybernétiques

En substance, le maCERT est chargé de prévenir et de réagir en cas d'incidents de sécurité informatique. En amont, et pour rester au diapason de l'état de la menace, il assure une veille pour mettre à jour sa base de connaissance, particulièrement en ce qui concerne les nouvelles attaques, les nouveaux logiciels malveillants et les dernières vulnérabilités. En aval, il analyse et traite les incidents de sécurité en aidant à leur résolution. Pour assurer ses missions, le maCERT centralise les signalements d'atteintes à la sécurité, analyse les rapports concernés et apporte, au besoin, l'assistance nécessaire pour faire face aux cybers incidents.

Le maCERT apporte indéniablement une expertise avancée en matière de veille, supervision, analyse et réaction. L'objectif essentiel étant de disposer d'une connaissance de la situation et de

déterminer les priorités en matière de protection et d'intervention afin de lutter contre les activités malveillantes ciblant les réseaux de notre pays.

La fonction de veille, de détection et de réaction aux attaques informatiques s'appuie certes sur les ressources propres du maCERT, mais également sur un effort collectif de la communauté internationale. En effet, les frontières du cyberespace ne sont pas reconnues et les cyberattaques sont naturellement transfrontalières. Dans ce cadre, le maCERT a mis en place un large réseau de coopération qui lui permet d'échanger sur l'évolution de la menace cybernétique à l'échelle internationale.

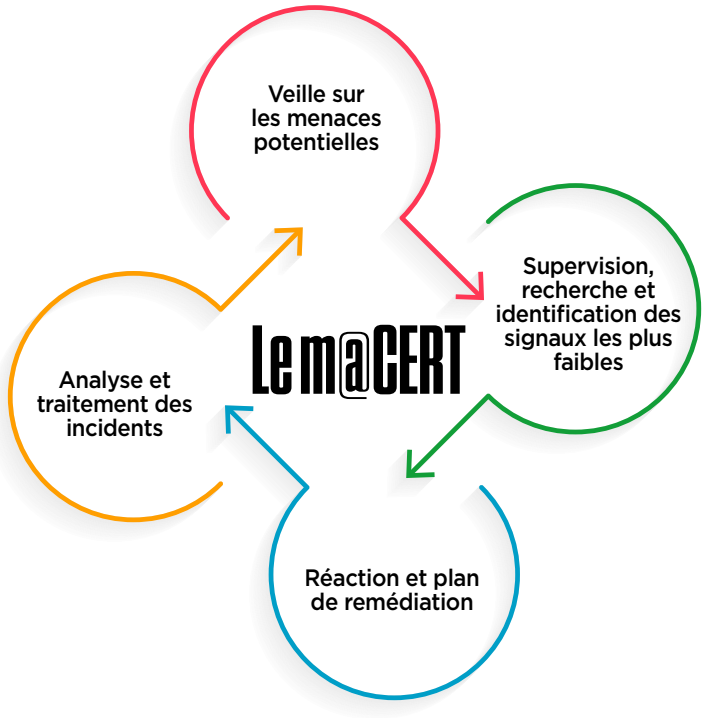
Le maCERT coopère en effet, avec ses homologues à l'étranger, notamment par le biais du FIRST (Forum of Incident Response and Security Teams), qui est un forum mondial qui regroupe plus de 400 CERTs, dans lequel les différentes équipes de réponse aux incidents cybernétiques peuvent partager l'information et les bonnes pratiques. Il coopère aussi, sur un plan bilatéral, avec les CERTs des pays partenaires qui ont conclu avec la DGSSI des accords de coopération.

Le m@CERT..une structure intégrée et cohérente, à l'affût de tout signal révélateur

Le maCERT est constitué de quatre équipes, dont les missions sont détaillées ci-dessous:

L'équipe de veille

Elle assure une recherche continue sur les menaces et attaques susceptibles de cibler le cyberespace national, car chaque jour, de nouveaux risques et de nouvelles vulnérabilités sont découvertes et publiées sur Internet. Le maCERT doit avertir au plus tôt ses parties prenantes afin de mettre en place les contre-mesures appropriées. Cette équipe dispose d'outils adaptés et puise des informations pertinentes dans les sites web spécialisés, les forums, chez les éditeurs de logiciels et les partenaires. La veille permet au maCERT de rester au diapason des menaces émergentes (Threat Intelligence) qui pourraient cibler le cyberespace national et de collecter des informations sur les nouvelles vulnérabilités. Ces informations sont ensuite disséminées par différents moyens à l'ensemble des responsables de sécurité des systèmes d'information (RSSI) des administrations, organismes publics et infrastructures d'importance vitale



L'équipe de supervision

Elle a pour mission de rechercher et d'identifier de manière continue les signes et prémisses des nouvelles menaces et attaques qui ciblent les systèmes d'information des départements supervisés par le maCERT. Cette action consiste essentiellement en la collecte, l'analyse et la qualification des événements de sécurité produites par les solutions de supervision afin de détecter tous les types de cyber menaces et incidents susceptibles d'affecter les systèmes d'information des ministères, administrations publiques et infrastructures d'importance vitale. Les solutions de supervision et de détection des incidents de sécurité sont installées au niveau des nœuds Internet des parties prenantes et permettent de superviser l'ensemble des domaines et adresses publiques des entités marocaines. Une fois ces données analysées et stockées dans une base de données «Big Data », des outils intelligents procèdent à leur corrélation, en se basant sur des signatures et des règles de sécurité régulièrement mises à jour.

L'équipe d'analyse

Elle traite les incidents et requêtes remontés par les équipes de veille et de supervision ainsi que ceux déclarés par les parties prenantes. Cette analyse peut prendre plusieurs aspects : rétro-ingénierie ou ingénierie inverse des codes malveillants, évaluation dynamique des logiciels

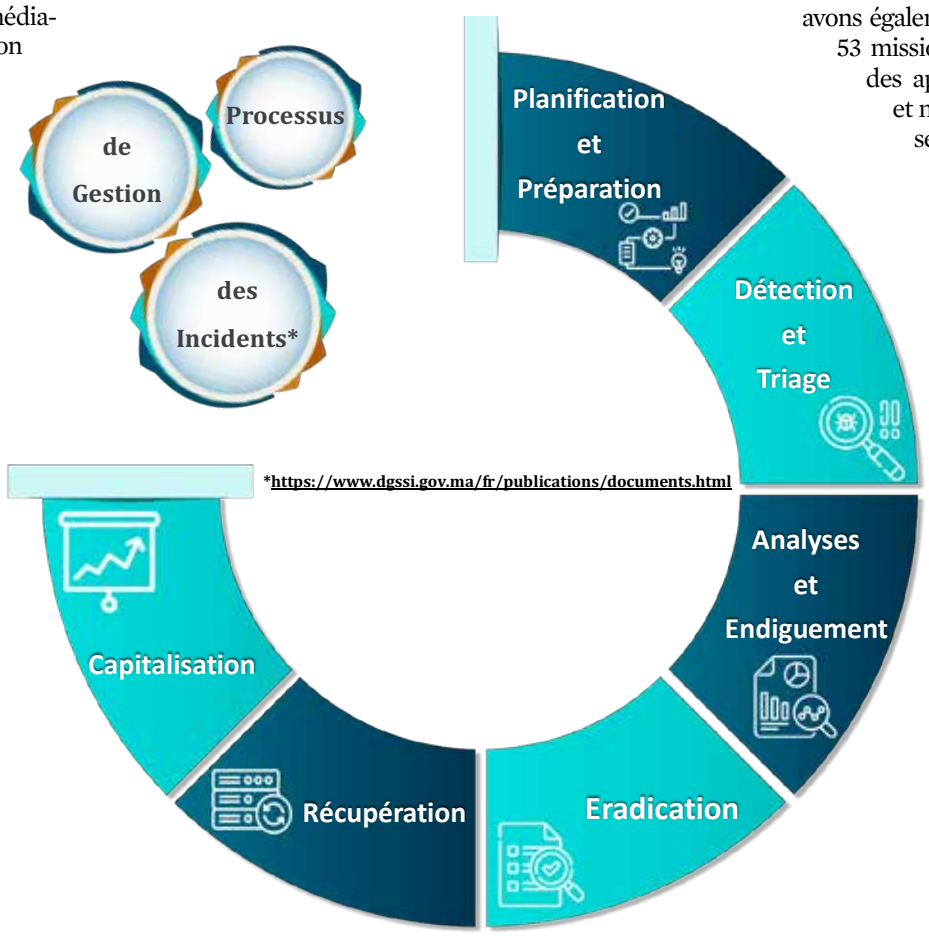
malicieux, analyse du trafic réseau et des journaux des applications, etc.

La capacité d'analyse comprend une solution de gestion des informations et des événements de sécurité, des outils de capture de paquets, un laboratoire d'analyse des logiciels malveillants, des outils de visualisation des flux, des outils de gestion et de réponse aux incidents et des bases de données « Big data » qui permettent l'analyse de volumes importants de données.

Ces services d'analyse et de test permettent d'identifier les vulnérabilités dans les réseaux des parties prenantes et les rapports d'analyse des risques avec des recommandations de remédiation élaborés à cet effet permettent une atténuation proactive des risques exploitables.

L'équipe de réaction

Elle procède, après l'analyse d'un cyber-incident, à la reconstitution du scénario d'attaque et élabore un plan de remédiation. Elle dirige et coordonne, conformément à ce plan, le lancement, le rétablissement du fonctionnement normal des services et/ou des réseaux infectés. Ce plan comprend notamment les recommandations et mesures à prendre afin de corriger les failles détectées et durcir la sécurité des systèmes infectés. Elle peut aussi assister les parties concernées à implémenter ces recommandations. Une fois la mise en œuvre du plan de remédiation achevée, une évaluation du nouveau système de protection est lancée afin de tester si les recommandations émises ont bien été implémentées.



*https://www.dgssi.gov.ma/fr/publications/documents.html

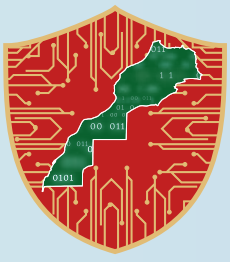
Le m@CERT.. une efficacité opérationnelle 24h/24 et 7j/7

L'année 2021 a été marquée par de nombreuses cybermenaces et d'activités malveillantes détectées par le maCERT et rapidement prises en charge, qui ont épargné à notre pays des dégâts divers, selon une approche d'analyse des incidents.

Grâce à l'activité dynamique de veille, 784 bulletins d'alerte de sécurité ont été produits et diffusés. Quant aux activités de supervision des domaines, adresses IP publiques et autres systèmes exposés sur Internet de l'ensemble des ministères, administrations publiques et infrastructures vitales, elles ont permis de détecter 342 cybermenaces et activités malveillantes. D'autres types d'alertes concernent la divulgation des données sur Internet, de problèmes de mal-configuration au niveau des réseaux, des infections des machines par des malwares ou encore la publication d'informations à caractère personnel sur Internet. Ces actions ont engagé des alertes et recommandations transmises aux parties concernées, pour prendre les mesures idoines.

En ce qui concerne les activités d'analyse et de réaction, nous avons pu traiter 246 incidents déclarés. Nous avons également pu réaliser 53 missions d'évaluation des applications Web et nous avons diffusé 50 alertes, suite aux scans réalisés régulièrement ■

Bilan des activités du m@CERT
durant l'année 2021



Activités de Veille

568
Notes d'information et bulletins d'alerte de sécurité

43
Bulletins concernaient des failles de sécurité non encore découvertes ou n'ayant pas encore reçu de correctifs

173
Bulletins à caractère "CRITIQUE"

Activités de Supervision

265
Cybermenaces détectées grâce à la supervision des domaines, adresses IP publiques et systèmes exposés sur internet de l'ensemble des ministères, administrations publiques et infrastructures d'importance vitale.

Alertes et recommandations transmises aux parties concernées

77
Activités malveillantes détectées aux niveaux des parties prenantes supervisées par le **maCERT**

Autres types d'alertes concernant la divulgation des données d'authentification sur internet, des problèmes de mal-configuration aux niveau des réseaux, des infections des machines par malwares ou encore la publication d'information à caractère personnel sur internet

Activités d'Analyse et de Réaction

246
Cyber-Incidents déclarées et traitées par le **maCERT**

53
Missions d'évaluation d'applications web

50
Alertes diffusées suite aux scans réalisés régulièrement par le **maCERT**

Entretien avec

M. Saâd EL KHADIRI

le Directeur de la Stratégie et de la Réglementation à la Direction Générale de la Sécurité des Systèmes d'Information

La cybersécurité.. une démarche stratégique, cohérente et intégrée

La Revue de Police s'est rendue au siège de la DGSSI et s'est entretenue avec les responsables de cette structure stratégique, pour éclairer le lectorat sur les missions et réalisations de cette Direction Générale, qui constitue un vrai rempart contre les cyberattaques, afin de renforcer la confiance et la résilience de nos Systèmes d'Information les plus vitaux.

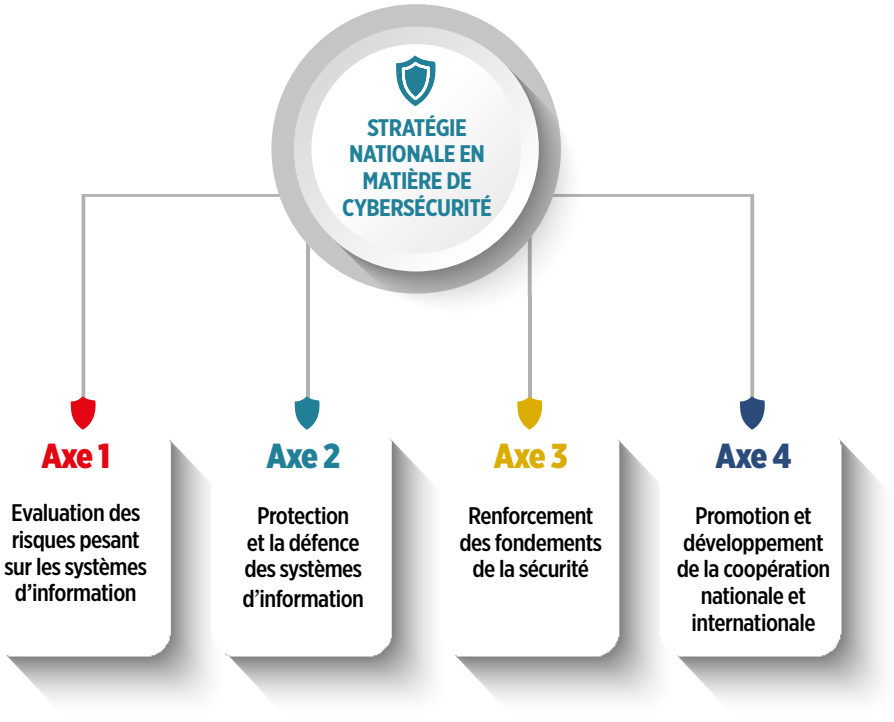
Quelle est la Stratégie Nationale de la Cybersécurité ?

Il faut dire que depuis 2009, le Maroc a lancé, sous la présidence effective de **Sa Majesté le ROI, que Dieu L'assiste,** la stratégie « Maroc Numeric 2013», qui a retenu la confiance numérique et la cybersécurité en tant que mesures d'accompagnement indispensables à l'ancrage du Maroc à l'économie numérique.
Dans ce contexte, et à l'instar de ce qui se fait à l'international, la première stratégie nationale de la cybersécurité (SNC) a été adoptée en décembre 2012. Cette stratégie nationale a pour vocation de doter les systèmes d'information nationaux d'une capacité de défense et de résilience, à même de créer les conditions d'un environnement de confiance et de sécurité, propice au développement de la société de l'information. Ladite stratégie repose sur quatre axes stratégiques :

- L'évaluation des risques pesant sur les systèmes d'information au sein des administrations, organismes publics et infrastructures d'importance vitale ;
- La protection et la défense des systèmes d'information des administrations, organismes publics et infrastructures d'importance vitale ;
- Le renforcement des fondements de la sécurité : Cadre juridique, Sensibilisation, Formation et Recherche & Développement ;
- La promotion et le développement de la coopération nationale et internationale.

Quelles sont les réalisations découlant de la mise en œuvre de cette stratégie ?

L'implémentation de la stratégie nationale, ainsi que les plans d'action annuels, ayant reçu **le Haut Assentiment de Sa Majesté le ROI, que Dieu L'assiste,** qui en ont découlés ont largement contribué à la mise à niveau de l'arsenal juridique et normatif régissant la cybersécurité. Il s'agit en particulier des lois sur la cybersécurité, sur les services de confiance pour les transactions électroniques et de la Directive Nationale de la Sécurité des Systèmes d'Information «DNSSI». Cette mise à niveau a eu un impact significatif sur la protection du cyberespace national et sur le développement de la confiance numérique, et qui constituent des préalables au développement de l'écosystème digital.
Dans le même sillage, la stratégie susvisée a permis d'améliorer l'offre de formation au profit des départements de l'Etat et d'organiser diverses actions de sensibilisation sur les enjeux de la cybersécurité. La SNC a ainsi contribué au renforcement de la résilience des systèmes d'information nationaux, à travers l'amélioration de l'aptitude des organismes publics et des organismes gérant des infrastructures d'importance vitale à détecter rapidement les cyberattaques et à les contenir, en les encourageant à mettre en place des centres



L'implémentation de la stratégie nationale, ainsi que les plans d'action annuels, ayant reçu le Haut Assentiment de ***Sa Majesté le ROI, que Dieu L'assiste,*** *qui en ont découlés ont largement contribué à la mise à niveau de l'arsenal juridique et normatif régissant la cybersécurité.*

Evaluation des risques pesant sur le cyberespace national

- Dresser une cartographie des SI nationaux
- Identifier les SI sensibles
- Promouvoir la culture d'évaluation périodique de la sécurité

opérationnels de sécurité (SOC) et à coordonner la réaction auxdites attaques avec le centre de veille, détection et réponse aux attaques informatiques (maCERT) relevant de la DGSSI.

Dans le cadre de l'évaluation des risques pesant sur le cyberspace national, la stratégie nationale de cybersécurité a permis de dresser une cartographie des systèmes d'information nationaux et d'identifier les systèmes d'information considérés sensibles pour l'Etat. En outre, les missions d'audit menées par la DGSSI ont favorisé le développement d'un cadre propice à la promotion de la culture d'évaluation périodique de la sécurité.

Concernant le volet de la coopération internationale, ladite stratégie a favorisé l'établissement et la signature de plusieurs accords de partenariat avec des organismes étrangers. Ces accords, qui couvrent notamment la dimension relative à la gestion des incidents de cybersécurité, mettent l'accent sur l'échange de l'information, de l'expertise et des bonnes pratiques.

Etant donné la nécessité de mettre à jour la stratégie nationale de cybersécurité, la DGSSI a lancé en 2021 deux études préliminaires portant sur l'évaluation de la maturité et des risques cybernétiques au niveau national en adoptant une approche participative via la consultation de dizaines d'experts et d'organismes concernés par la thématique de la cybersécurité. Les enseignements et conclusions tirées lors de ces deux études constitueront un préalable, permettant de concevoir une stratégie de cybersécurité adaptée à notre contexte et répondant à l'évolution rapide du paysage numérique et à la complexité croissante des risques cybernétiques.

Enfin, il sied de préciser que le Royaume du Maroc a pu enregistrer une progression au classement de l'index global de cybersécurité « GCI» de l'Union internationale des télécommunications (UIT) pour se hisser, entre 2018 et 2020, du 93ème au 50ème rang à l'échelle mondiale, grâce aux efforts consentis dans le cadre de la mise en œuvre de la stratégie nationale.

POLICE

Quels sont les organes de gouvernance de la cybersécurité au Maroc?

Le Comité stratégique de la cybersécurité

Créé par la loi n°05-20 relative à la cybersécurité, le comité stratégique de la cybersécurité, anciennement appelé le comité stratégique de la sécurité des systèmes d'information, est chargé d'élaborer les orientations stratégiques de l'Etat en matière de cybersécurité et veiller sur la résilience des systèmes d'information des entités, des infrastructures d'importance vitale et des opérateurs. Il est responsable de l'évaluation annuelle du bilan d'activité de la DGSSI et des travaux du comité national de gestion des crises et évènements cybernétiques majeurs. Par ailleurs, il arrête le périmètre des audits de la sécurité des systèmes d'information effectués par la DGSSI.

Ledit comité soutient également l'instauration de programmes et d'actions de sensibilisation et de renforcement des capacités

Organes de gouvernance de la SSI

Comité stratégique de la Cybersécurité

Créé par l'article 35 de la loi 05-20
Définit les orientations stratégiques de l'Etat en matière de Cybersécurité

Autorité Nationale de la Cybersécurité
(DGSSI relevant de l'Administration de la Défense Nationale)

Mise en œuvre de la stratégie de l'Etat dans le domaine de la cybersécurité

Centre de veille, détection et réponse aux attaques informatiques (maCERT)

Comité de gestion des crises et événements cybernétiques majeurs

© 2021 DGSN

en cybersécurité au profit des entités et des infrastructures d'importance vitale.

Enfin, il est chargé de donner son avis sur les projets de textes législatifs et réglementaires se rapportant au domaine de la cybersécurité.

Le Comité de gestion des crises et événements cybernétiques majeurs

Institué, auprès du comité stratégique de la cybersécurité, le comité de gestion des crises et évènements cybernétiques majeurs est chargé d'assurer une intervention coordonnée en matière de prévention et de gestion de crise par suite d'incidents de cybersécurité. Il peut décider des mesures que les entités et les responsables des infrastructures d'importance vitale doivent mettre en œuvre et élaborer des recommandations et conseils destinés aux opérateurs du secteur privé et aux particuliers.

A cet effet, les exploitants des réseaux publics de télécommunications, les fournisseurs d'accès à Internet, les prestataires de services de cybersécurité et les prestataires de services numériques sont tenus, en cas de crises cybernétiques majeures, de répondre aux prescriptions et demandes de concours et d'assistance technique du comité de gestion des crises et évènements cybernétiques majeurs.

> *Le comité de gestion des crises et évènements cybernétiques majeurs est chargé d'assurer une intervention coordonnée en matière de prévention et de gestion de crise par suite d'incidents de cybersécurité*

La Directiong Générale de la Sécurité des Systèmes d'Information (DGSSI)

La DGSSI est l'autorité nationale de la cybersécurité chargée de mettre en œuvre la stratégie de l'Etat en matière de cybersécurité. Elle est aussi chargée, notamment, d'élaborer des projets de textes de lois et de règlements en rapport avec la cybersécurité, de définir des mesures de protection des systèmes d'information et de veiller à leur application en assistant et conseillant les entités et les infrastructures d'importance vitale lors de leur mise en place. Par ailleurs, elle est responsable de la qualification des prestataires d'audit des systèmes d'information et ceux de service de cybersécurité.

En outre, la DGSSI a pour mission de mettre en place, en relation avec les entités et les infrastructures d'importance vitale, un système externe de veille, de détection et d'alerte des événements susceptibles d'affecter la sécurité de leurs systèmes d'information et coordonner la réaction à ces événements.

(maCERT)

Centre de veille, de détection et de réponse aux attaques informatiques

Le maCERT est l'une des directions de la DGSSI. Il est chargé de la mise en œuvre, en relation avec les autres administrations, de systèmes de veille, de détection, d'alerte des événements susceptibles d'affecter la sécurité des systèmes d'information de l'Etat et de la coordination de la réaction à ces événements.

Acteur essentiel à l'instauration de la confiance numérique, le centre procède également à la diffusion régulière de bulletins de sécurité et de

MaCERT..opérationnel 24/24 et 7j/7, à l'affût de tout signal aussi minime soit-il

Evolution du cadre réglementaire et institutionnel régissant la Cybersécurité au Maroc

2011
- Création du Comité Stratégique de la SSI (CSSSI)
- Création de la DGSSI
- Création du maCERT

2012
Adoption de la Stratégie Nationale de Cybersécurité

2014
Publication de la Directive Nationale de la Sécurité des Systèmes d'Information « DNSSI »

© 2021 DGSN

vulnérabilités, d'alertes et de notes d'information. Ces bulletins ont pour objectif d'avertir les intéressés des éventuels risques et menaces qui pourraient les atteindre.

Enfin, le maCERT propose un service d'assistance à la réponse aux incidents de sécurité cyber. Il incite toutes les Administrations, Organismes publiques et Infrastructures d'importances vitales à déclarer tout incident de sécurité cyber.

POLICE

Qu'en est-il du cadre juridique et réglementaire national ? Est-il adapté aux nouveaux enjeux de la cybersécurité et est-il conforme aux standards internationaux régissant ce domaine ?

Les enjeux liés à la cybersécurité ont toujours constitué une partie intégrante des stratégies de digitalisation. Sur le plan réglementaire, une dynamique soutenue a été engagée pour la mise en place d'un cadre réglementaire étoffé couvrant tous les aspects autour de cette thématique, qu'est la cybersécurité.

En décembre 2012, la stratégie nationale de la cybersécurité a été adoptée. Elle a pour objectif de doter les systèmes d'information nationaux d'une capacité de défense et de résilience afin de créer les conditions d'un environnement de confiance et de sécurité, propice au développement de la société de l'information.

En 2014, la DGSSI a élaboré la Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI) dans l'optique de rendre opérationnelles les orientations inscrites dans la stratégie nationale de cybersécurité. Cette directive intervient pour élever et homogénéiser le niveau de protection et de maturité de la sécurité de l'ensemble des systèmes

DNSSI.. un référentiel national de cybersécurité

La Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI) a été publiée en 2014 par circulaire du Chef de Gouvernement. L'objectif étant d'élever et d'homogénéiser le niveau de protection et de maturité de la sécurité de l'ensemble des systèmes d'information des administrations et organismes publics, ainsi que des infrastructures d'importance vitale.

Une période transitoire de trois années a été accordée aux parties concernées, pour se mettre en conformité avec cette directive.

La DNSSI s'appuie sur un ensemble de règles, procédures et/ou bonnes pratiques reconnues au plan international, dont la norme ISO/CEI 27002 dans sa version 2009.

Elle s'organise à ce titre sous forme de 11 chapitres:

- Politique de sécurité de l'information ;
- Organisation de la sécurité ;
- Gestion des biens ;
- Sécurité liée aux ressources humaines ;
- Sécurité physique et environnementale;
- Gestion de l'exploitation et des télécommunications ;
- Contrôle d'accès;
- Acquisition, développement et maintenance ;
- Gestion des incidents;
- Gestion du plan de continuité de l'activité;
- Conformité.

2016 — Décret n°2-15-712 fixant le dispositif de protection des systèmes d'information sensibles des infrastructures d'importance vitale

2018 — Arrêté du Chef du Gouvernement fixant les critères d'homologation des prestataires d'audit des Systèmes d'Information Sensibles des infrastructures d'importance vitale et les modalités de déroulement de l'audit

2020 — Loi n° 05-20 relative à la Cybersécurité
Loi n°43-20 relative aux services de confiance pour les transactions électroniques

2021 — Décret d'application de la loi n° 05-20 relative à la Cybersécurité

d'information des administrations et organismes publics ainsi que des infrastructures d'importance vitale, en précisant les mesures de sécurité organisationnelles et techniques applicables.

En mars 2016, le décret n° 2-15-712 fixant le dispositif de protection des systèmes d'information sensibles des infrastructures d'importance vitale a été adopté. Ce décret définit les règles applicables pour renforcer la résilience et garantir la continuité de fonctionnement des systèmes d'information des infrastructures d'importance vitale. Ces infrastructures, pour rappel, englobent les installations, ouvrages et systèmes qui sont indispensables au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social, et dont le dommage ou l'indisponibilité ou la destruction aurait un impact induisant la défaillance de ces fonctions.

Sur un autre registre, et afin de donner un élan au développement des activités d'audit des systèmes d'information sur le territoire national, un arrêté du Chef du Gouvernement a été élaboré en 2018 pour fixer les critères d'homologation des prestataires d'audit des Systèmes d'Information Sensibles des infrastructures d'importance vitale et les modalités de déroulement de l'audit. Cette homologation repose sur un certain nombre de prérequis exigés des prestataires, notamment en matière de compétences, d'expertises et de qualité de service.

En 2020, l'arsenal juridique a été enrichi par la promulgation de deux textes législatifs ayant un impact significatif sur la protection du cyberespace national et sur le développement de la confiance numérique, constituant ainsi les préalables au développement de l'écosystème digital. Il s'agit de la loi n° 05-20 relative à la cybersécurité et de la loi n°43-20 relative aux services de confiance pour les transactions électroniques.

Dans la continuité des efforts déployés dans le domaine juridique, l'année 2021 a été marquée par la publication du décret d'application de la loi n° 05-20 relative à la cybersécurité. Ce texte fixe la composition et les modalités de fonctionnement des organes de gouvernance de la cybersécurité, prévus par la loi n° 05-20, à savoir l'autorité nationale de la cybersécurité, le comité stratégique de la cybersécurité et le comité de gestion des crises et évènements cybernétiques majeurs. Ledit décret détaille les dispositions propres aux entités disposant de systèmes d'information sensibles, et aussi celles relatives aux opérateurs (exploitants des réseaux publics de télécommunication, fournisseurs d'accès à Internet, prestataires de services de cybersécurité, prestataires de services numériques et éditeurs de plateformes Internet). Enfin, il détermine les critères de qualification des prestataires de services d'audit et de cybersécurité.

Il sied de préciser enfin que la DGSSI, conformément à ses attributions, a élaboré et publié plusieurs directives, règlements, guides et référentiels en rapport avec la cybersécurité, et ce, afin d'accompagner les administrations de l'Etat, les établissements publics et les infrastructures d'importance vitale à renforcer la sécurité et la résilience de leurs systèmes d'information ■

La loi n° 05-20 relative à la cybersécurité promulguée par le dahir n° 1-20-69 du 4 hija 1441 (25 juillet 2020)

La loi n° 05.20, élaborée suite aux Hautes Instructions Royales, vient couronner un important processus de mise sur pied de notre dispositif juridique national relatif à la cybersécurité. Elle a pour vocation de mettre en place les fondamentaux nécessaires à même de favoriser la digitalisation et développer la confiance numérique dans notre pays.

Cette loi, adoptée en Conseil de Ministres le 06 juillet 2020, a pour objectif d'instaurer les mesures de protection et de résilience des systèmes d'information des administrations de l'Etat, des collectivités territoriales, des établissements et entreprises publics et de toute autre personne morale de droit public.

Outre le dispositif de droit commun, les infrastructures d'importance vitale qui peuvent relever aussi bien du secteur public que du secteur privé, sont soumises, en vertu de la loi, à des règles complémentaires et spécifiques. Il s'agit notamment de l'identification et l'homologation de leurs systèmes d'information sensibles et la soumission desdits systèmes à des audits de sécurité menés par la DGSSI ou par un prestataire qualifié.

Cette loi préconise également des mesures de protection des réseaux et systèmes d'information relevant de certaines catégories d'acteurs privés. Il s'agit notamment des exploitants des réseaux publics de télécommunications, des fournisseurs d'accès à internet, des prestataires de services de cybersécurité, des prestataires de services numériques ainsi que des éditeurs des plateformes internet.

La loi introduit une notion de classification des systèmes d'information basée sur l'analyse des impacts des incidents, susceptibles de porter atteinte aux besoins de sécurité en termes de disponibilité, intégrité et confidentialité. En fonction de cette classification, les systèmes d'information seront sujets à des mesures de protection définies par la DGSSI.

La loi prévoit aussi un mécanisme de partage et de collaboration entre la DGSSI et les services compétents de l'Etat permettant l'échange de toute donnée ou information susceptible d'aider dans le traitement des infractions portant atteinte aux systèmes de traitement automatisé des données. La DGSSI procède aussi à la saisine des autorités concernées lorsqu'il s'agit d'actes présumés contraires à la loi, révélés à l'occasion de l'exercice de ses attributions.

Compte tenu de la dimension transnationale des risques cybernétiques, la loi accorde un intérêt de premier plan au développement de la coopération avec les organismes nationaux et étrangers dans le domaine de la cybersécurité. Cette coopération permettra de favoriser le partage d'expérience et d'expertise dans ce domaine et de démultiplier ainsi les capacités de réponse aux cyberattaques.

Loi n° 43-20 relative aux services de confiance pour les transactions électroniques promulguée par le dahir n° 1-20-100 du 16 joumada I 1442 (31 décembre 2020)

A la faveur des différentes stratégies mise en œuvre, le Maroc affiche une ambition forte pour réussir sa transition numérique et tirer profit des opportunités offertes par le digital, comme véritable levier de croissance et de développement économique et social.

En effet, l'accélération du processus de digitalisation est considérée dans le cadre du nouveau modèle de développement comme l'un des objectifs prioritaires de l'action des pouvoirs publics. Afin d'accompagner ce choix stratégique, notre pays a misé sur le développement de la confiance numérique. Celle-ci constitue en effet un gage pour l'essor des services digitaux. La promotion et l'amélioration de la confiance et de la sécurité au profit des usagers : administrations, secteur privé et citoyens, sont en effet des facteurs clé de réussite.

Avec la promulgation de la loi n° 43-20 relative aux services de confiance pour les transactions électroniques, un pas important a été franchi dans ce sens. Cette loi, élaborée suite aux Hautes Instructions de **Sa Majesté le Roi**, couvre un large spectre de besoins et d'usages et permet de renforcer la confiance et d'encourager le recours à la dématérialisation.

En substance, cette loi adoptée en Conseil des Ministres le 14 octobre 2020, fixe le régime applicable aux services de confiance pour les transactions électroniques, aux moyens et prestations de cryptologie ainsi qu'aux opérations effectuées par les prestataires de services de confiance et les règles à respecter par ces derniers et par les titulaires des certificats électroniques.

La loi n° 43.20 a permis de lever les différents obstacles identifiés au développement du marché de la confiance numérique au Maroc dans la mesure où elle instaure trois niveaux de sécurité (simple, avancé et qualifié), ce qui permet la digitalisation de la majorité des usages : à faible, à moyen ou à fort enjeu. Elle introduit également le principe de non-discrimination en ce qui concerne l'effet juridique et la recevabilité en justice, en cas de recours aux services de confiance.La loi retient enfin un régime d'agrément au profit des prestataires privés qui désirent fournir des services de confiance qualifiés et un régime de déclaration pour les autres.

ENTRETIEN
avec

Le Colonel Major Abdellah BOUTRIG

Directeur de l'Assistance, de la Formation, du Contrôle et de l'Expertise à la DGSSI

Le contrôle, l'assistance et le renforcement des capacités nationales en matière de cybersécurité.. d'autres fonctions de la DGSSI

Pouvez-vous nous décrire les activités de la DGSSI en matière d'audit et de contrôle ?

L'audit de sécurité est un mécanisme de gouvernance qui permet de fournir une assurance raisonnable au commanditaire quant à la maîtrise des risques pouvant affecter la disponibilité du système d'information, l'intégrité des données ou leur disponibilité. C'est aussi une démarche qui permet de connaître le niveau de résilience et de protection globale de son système d'information. Il s'agit de contrôler l'efficacité des dispositifs mis en place, d'évaluer la pertinence des systèmes de surveillance et d'alerte et d'indiquer si les mesures de sécurité organisationnelles et techniques instaurées au sein de l'organisation sont efficaces.

Au niveau national, *l'importance de l'audit a été consacrée à travers les dispositions de la loi 05.20 relative à la cybersécurité et la Directive Nationale de la Sécurité des Systèmes d'Information «DNSSI»*.

Conformément à ces dispositions, les administrations de l'État, les collectivités territoriales, les établissements et entreprises publics et toute autre personne morale de droit public doivent régulièrement, auditer la sécurité de leurs systèmes d'information et se conformer à minima aux exigences de la «DNSSI».

A ce titre, l'une des missions fondamentales de la DGSSI est d'assurer les audits de sécurité des systèmes d'information aux profits des entités publiques et privées. L'objectif étant de s'assurer de l'efficacité des mesures de sécurité mises en place, de constater les écarts entre les mesures appliquées et celles normalement requises pour une bonne prise en charge des risques en matière de sécurité de l'information et de formuler, le cas échéant, des recommandations en vue de corriger les écarts repérés.

Afin de préserver le caractère impartial et la qualité des audits de sécurité effectués dans un cadre réglementaire, la loi 05.20 préconise qu'ils soient effectués soit par la DGSSI ou par des prestataires qualifiés à ce titre, particulièrement lorsqu'il s'agit de systèmes d'information sensibles appartenant à des Infrastructures d'Importance Vitale.

Quels sont alors, les différents types d'audits réalisés par la DGSSI?

La DGSSI opère selon un programme d'audits dont le périmètre et les modalités d'exécution sont arrêtés annuellement par le Comité Stratégique de la Cybersécurité « CSC ». Les principales activités d'audit portent sur :

- La conformité à la règlementation, normes et directives en vigueur ;
- L'évaluation des vulnérabilités des applications Web;
- L'analyse des architectures et les audits des configurations.

La DGSSI peut mener des audits de conformité et des audits techniques.

En quoi consiste l'audit de sécurité informatique ?

Le développement du digital, l'interconnexion des réseaux et des systèmes sont tout autant de facteurs qui multiplient les risques informatiques au sein des organisations.

Qu'il s'agisse de risques internes (manque de sensibilisation des collaborateurs, erreurs et incidents, accès aux données critiques, malveillance,...) ou de risques externes (virus, intrusions, phishing, espionnage...), la sécurité du système d'information est désormais un enjeu de taille dans la gouvernance de toute structure.

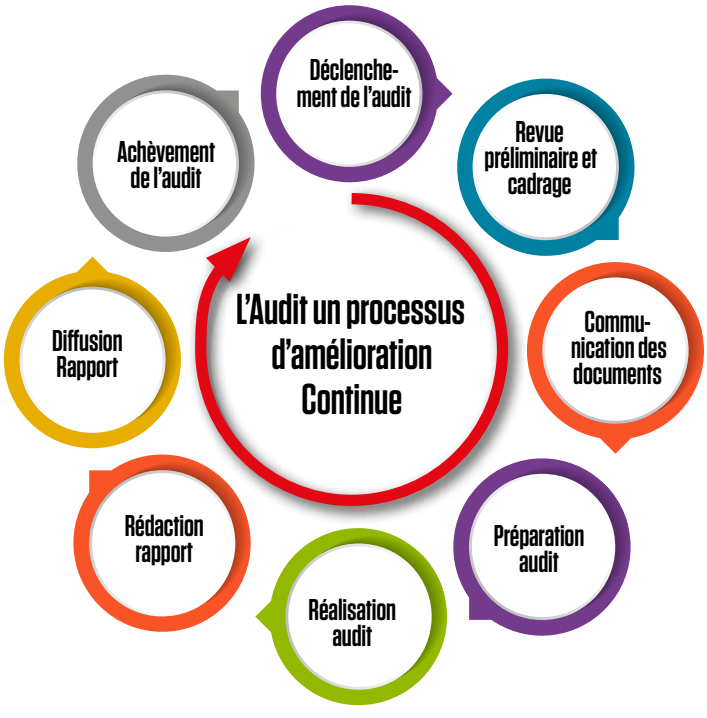
L'audit de sécurité est utilisé pour :

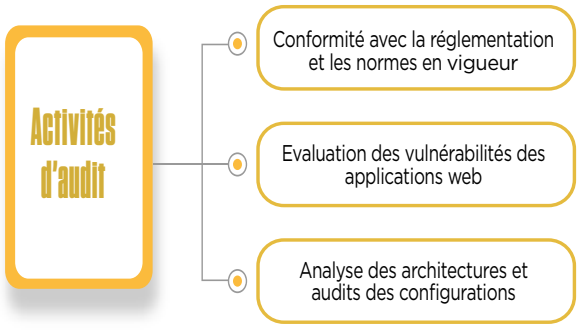
- s'assurer de l'intégrité des données et du capital informationnel de l'organisation;
- découvrir et comprendre les éventuelles vulnérabilités du système d'information;
- mettre en place des politiques de protection et de sécurité adaptées au fonctionnement de l'organisation et à son système d'information.

Dans un audit de sécurité informatique, sont étudiés, entre autre, les éléments suivants :

- le matériel : postes fixes, ordinateurs portables, tablettes, téléphones mobiles;
- les systèmes d'exploitation : leurs versions, leurs mises à jour;
- les logiciels et applications (logiciels de gestion, logiciels métiers, messagerie...);
- l'infrastructure réseaux et télécom;
- les risques associés à une éventuelle perte d'intégrité des données ;
- les droits et accès des collaborateurs;
- les besoins en matière de sauvegardes (hébergées, redondantes..);
- les outils de sécurité informatique (antivirus, pare-feux, antispam);
- la politique de sécurité informatique de l'entreprise;
- les dispositifs de sécurité externes; etc.

Si besoin, des tests d'intrusions peuvent être réalisés pour compléter l'audit de sécurité.





Concernant **les audits de conformité**, ils ont été initiés en 2017 par les équipes d'audit de la DGSSI suite à l'expiration de l'échéance des trois années probatoires consacrées à l'implémentation de la DNSSI, les audits de conformité à cette directive ont représenté un moyen idoine pour mesurer le niveau d'efficacité des mesures de sécurité implémentées par les parties prenantes.

L'objectif de ces audits était d'identifier d'une part le niveau de conformité des systèmes d'information audités aux exigences de sécurité organisationnelles et techniques édictées par la directive précitée, et d'autre part de relever les constats de non-conformité et de fournir des recommandations à même d'améliorer la sécurité des systèmes d'information des entités auditées.

Nous réalisons également ***des audits techniques,*** qui sont orientés principalement vers l'analyse des architectures et l'audit des configurations en place.

Les audits d'architecture consistent en la vérification de la conformité des pratiques de sécurité relatives au choix, au positionnement et à la mise en œuvre des dispositifs matériels et logiciels déployés dans un système d'information à l'état de l'art.

Les audits de configuration en revanche ont pour objectif la vérification de l'implémentation des bonnes pratiques de sécurité au niveau des configurations des actifs informationnels. Ces actifs peuvent notamment être des équipements réseau, des systèmes d'exploitation (serveur ou poste de travail), des applications ou des produits de sécurité.

Les audits techniques se basent sur les référentiels internationaux, les guides de bonnes pratiques élaborés par les éditeurs des différentes solutions technologiques ainsi que les guides de durcissement des configurations élaborés par la DGSSI. L'objectif étant de s'assurer de l'implémentation d'une défense en profondeur au niveau du système d'information et de réduire au maximum la probabilité d'occurrence de tout incident de sécurité ou événement indésirable.

Les audits précités (conformité et technique) sont sanctionnés par des rapports adressés aux top management des entités auditées, et dont les recommandations doivent faire l'objet de plans d'action de remédiation permettant in fine de relever le niveau de protection et de maturité de la sécurité de leurs systèmes d'information.

Depuis 2017, la DGSSI a mené une centaine de missions d'audit au profit de plusieurs ministères, établissements publics et infrastructures d'importance vitale. Grâce à des comptes rendus détaillés adressés aux responsables des entités auditées à l'issue des audits (conformité et technique), les parties prenantes sont en mesure de différencier les risques «acceptables» de ceux qui ne le sont pas. Des recommandations sont également proposées afin de placer le bon niveau de prévention sur l'ensemble des risques identifiés et établir des plans d'action pour la remédiation. La DGSSI contribue également par l'assistance à la mise en œuvre des recommandations lorsque le besoin se présente.

POLICE

Quelle évaluation faites-vous des vulnérabilités des systèmes exposés sur le Web?

Les actions d'évaluation des vulnérabilités ont pour but de déceler la présence de failles dans les systèmes d'informations exposés au public et principalement les plateformes web. Ces évaluations sont généralement sollicitées par les parties prenantes avant la mise en ligne des plateformes ou suite à un changement significatif dans leurs environnements d'hébergement. Elles peuvent aussi intervenir à l'initiative de la DGSSI, suite à l'apparition de nouvelles menaces.

Les vulnérabilités les plus récurrentes cette année sont :

- Exposition des données au public (navigation dans les répertoires, exposition du code source des applications et de l'interface d'administration) ;

- Mauvaise gestion d'accès ;
- Possibilité d'exploitation de failles de sécurité des applications interagissant avec des bases de données (Injection SQL) ;
- Faibles politiques de gestion des mots de passe.

L'exploitation malveillante d'une seule ou de plusieurs de ces vulnérabilités pourrait conduire à l'une des attaques ci-après :

- Défiguration de site web ;
- Utilisation des plateformes pour abriter et distribuer des codes malicieux ;
- Accès illicite aux données ;
- Contrôle total sur les serveurs abritant l'application Web et possibilité de l'utiliser comme point de rebond pour atteindre le réseau interne.

A l'issue de toute évaluation, un rapport détaillant les vulnérabilités décelées, les risques potentiels engendrés, ainsi que les recommandations pour y remédier est transmis à la partie prenante. Ces recommandations ont généralement trait au renforcement des pratiques de développement et de déploiement sécurisés. La DGSSI effectue une réévaluation après l'implémentation des recommandations.

Qualification des PASSI/PSC

Afin de donner un élan au développement des activités d'audit et de contrôle des systèmes d'information dans notre pays, la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) a mis en place, via la loi n°05-20 relative à la cybersécurité et son décret d'application n°2-21-406, un régime de qualification destiné aux prestataires d'audit de la sécurité des systèmes d'information (PASSI) et aux prestataires de service de cybersécurité (PSC), désirant fournir leurs services au profit des infrastructures d'importance vitale, disposant de systèmes d'information sensibles.

Le processus de qualification se déroule conformément au décret n°2-21-406 pris pour l'application de la loi 05.20 relative à la cybersécurité. Dans le cadre de ce processus, les prestataires sont appelés à se soumettre à des évaluations menées par la DGSSI ou par des organismes désignés, et ce, conformément à des référentiels d'exigences élaborés par ladite direction générale, et qui consistent en un ensemble de règles qui s'imposent aux prestataires qui désirent obtenir une qualification de leurs services. Les évaluations portent notamment sur la vérification :

- Des connaissances et compétences des auditeurs et experts candidats ;
- Des processus du prestataire candidat (veille, formation et maintien des compétences, gestion des ressources, moyens de travail et outils etc.) ;
- De la sécurité des locaux et du système d'information du prestataire candidat ;
- Des méthodologies de travail et des outils utilisés.

La qualification constitue un gage de confiance et permet aux commanditaires de disposer de garanties sur la compétence des prestataires et de leur personnel, sur la qualité de la prestation et sur la confiance qui peut leur être accordée.

POLICE

Quelles sont les autres prestations que peut offrir la DGSSI aux parties prenantes?

En plus des audits de sécurité, la DGSSI mène depuis sa création des missions d'assistance à maîtrise d'ouvrage qui ont pour principal objectif d'accompagner les administrations, organismes publics et infrastructures d'importance vitale dans leurs projets de mise à niveau de la sécurité de leurs systèmes d'information. Ces actions se traduisent par l'aide à la rédaction des termes de référence, le suivi de l'exécution et de la qualité des prestations fournies ainsi que l'assistance à la validation des livrables.

La démarche d'assistance adoptée vise à aider les parties prenantes à mieux connaître leur environnement et ses vulnérabilités à travers l'analyse des risques, à identifier les mesures techniques et organisationnelles à appliquer pour réduire les risques potentiels, à définir et appliquer une politique et des procédures de sécurité afin de protéger leurs actifs informationnels et à vérifier régulièrement la conformité et l'efficacité des mesures en place avec la politique de sécurité.

POLICE

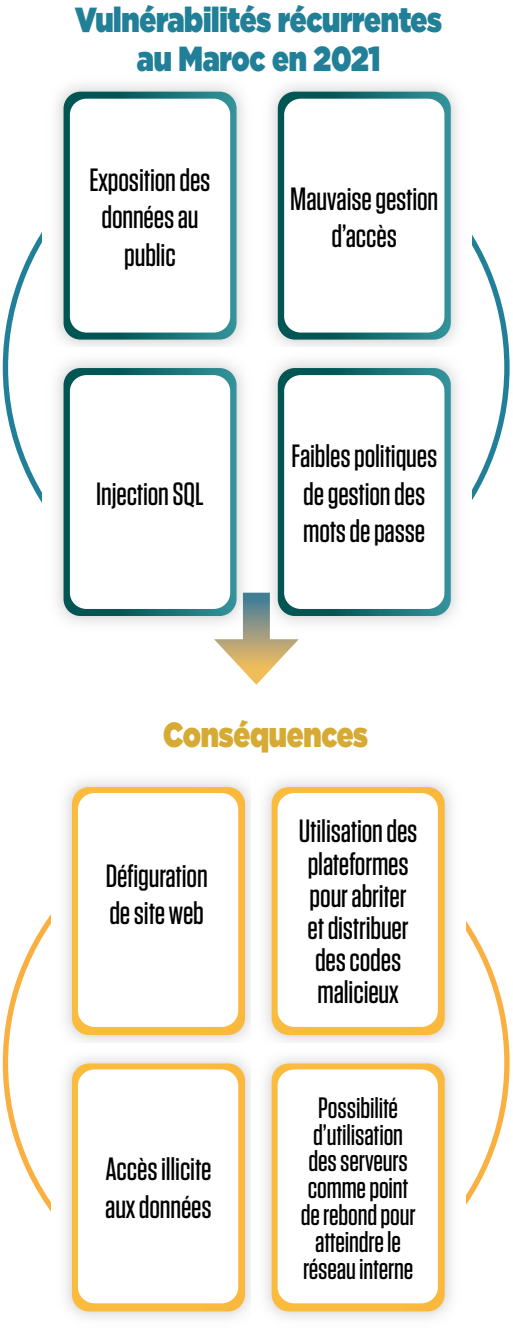
Vous êtes également responsable de la formation et du renforcement des capacités nationales en matière de cybesécurité. Quel est l'état des lieux ?

D'aucuns considèrent que l'humain représente le maillon faible de la chaîne de la cybersécurité. Les erreurs humaines et les actions malveillantes peuvent avoir des impacts considérables pour la sécurité des systèmes d'information de toute organisation. Avoir du personnel conscient et formé face à la cybermenace est essentiel afin de minimiser les risques émanant du cyberespace. Le facteur humain doit constituer le premier rempart contre les attaques informatiques.

La formation et le développement des compétences nationales est un pilier majeur de la stratégie nationale de la cybersécurité, sur lequel travaille acharnement la DGSSI, de concert avec d'autres départements nationaux, car la cybersécurité est d'abord et avant tout, une question de ressources humaines qualifiées capables

d'appréhender les risques cybernétiques pour mettre en place les process et les technologies adaptés pour s'en prémunir.

A ce titre, la formation et le développement des compétences nationales en matière de cybersécurité constituent des actions récurrentes des différents plans d'action de la DGSSI, et ce, depuis sa création en 2011. L'objectif étant d'instaurer une culture «cyber» au sein de l'écosystème national et de participer au développement de l'expertise nationale en matière de cybersécurité par la formation de cadres en mesure d'appréhender, dans toutes leurs dimensions, les problématiques liées à la sécurité des systèmes d'information.



Le renforcement des cybercompétences nationales.. une action des plus fondamentale de la stratégie nationale de cybersécurité.

En effet, cette direction générale met à contribution son réseau de coopération nationale et internationale pour initier des programmes de formation riches et diversifiés au profit de son personnel, mais également au profit du personnel de l'ensemble des départements ministériels, des établissements publics, des collectivités territoriales et des infrastructures d'importance vitale publiques et privées.

Aussi, dans un contexte particulier lié à la pandémie de la COVID-19, la DGSSI a su maintenir, voire renforcer la dynamique enclenchée depuis plusieurs années pour répondre aux besoins croissants en formation, et ce grâce au recours aux dispositifs e-learning et à l'activation du centre de formation de la DGSSI.

Dans ce cadre, 600 ingénieurs et responsables des systèmes d'information des départements étatiques et des infrastructures d'importance vitale ont bénéficié de formations proposées aussi bien dans le cadre du Master spécialisé en cybersécurité ou à l'occasion de formations mobilisées dans le cadre de la coopération internationale.

En effet, et compte tenu du besoin pressant de doter les organismes de l'Etat et du secteur privé en responsables de sécurité des systèmes d'information et répondre à l'une des exigences principales de la directive nationale de la sécurité des systèmes d'information (DNSSI), la DGSSI a mis en place depuis 2015, un Master spécialisé en cybersécurité au niveau de l'Institut National des Postes et Télécommunications (INPT), et ce, dans le cadre d'un partenariat avec l'Agence Nationale de Réglementation des Télécommunications (ANRT). Ce master met à contribution

des formateurs experts nationaux et étrangers pour dispenser un programme avancé qui s'inspire des cursus de formation développés par des universités et des instituts de formation de renom à l'échelle internationale.

A l'échelle internationale, La DGSSI met en œuvre, en partenariat avec des institutions homologues dans des pays étrangers ou en liaison avec des centres de formation de renommée internationale, des programmes de formation avancés en cybersécurité. Ces formations sont organisées au Maroc ou à l'Etranger et sont ouvertes aux ingénieurs nationaux disposant des prérequis nécessaires.

Outre ces programmes, des formations spécialisées de courte durée sont dispensées au niveau du centre de formation de la DGSSI, aussi bien par ses ressources propres que par de l'expertise apportée par les principaux acteurs de l'écosystème de cybersécurité.

Afin d'assurer l'apprentissage par la pratique, la DGSSI organise périodiquement des exercices cyber ***«Cyber drill»*** et envisage d'enrichir son offre de formation et de sensibilisation par le recours à une solution de simulation « Cyber Range » riche en fonctionnalités et scénarios de cyberattaques modernes. L'objectif de cette plateforme de simulation en cybersécurité, étant de permettre aux participants d'acquérir une meilleure compréhension des principales méthodologies, opérations et procédures de sécurité ainsi que les compétences et l'expertise nécessaires pour lutter contre les cybermenaces.

POLICE

Si la cybersécurité est l'affaire de tous, quel rôle joue la DGSSI en matière de sensibilisation des citoyens, pour plus de sécurité dans le cyberespace ?

Dans un monde hyperconnecté où les technologies de l'information et des communications rythment de plus en plus le quotidien de nos sociétés, les attaques cybernétiques ne cessent de se développer et de se perfectionner. Les cyberattaquants usent de techniques d'attaques avancées pour cibler les utilisateurs, les employés et les partenaires des organisations. Dès lors, la sensibilisation devient une priorité majeure et un facteur déterminant pour une meilleure protection de notre patrimoine informationnel.

Face à la complexité des cyberattaques, les organisations doivent mettre en place des plans de sensibilisation à plusieurs niveaux, aussi bien chez les utilisateurs des systèmes d'information, que chez les employés en général. La vigilance devra être de mise et tout le personnel, quel que soit sa responsabilité, devra être sensibilisé aux risques et aux menaces du cyberespace. Le but recherché ne se limite pas pour autant à la conformité, il concerne davantage la transformation de la culture de l'organisation en matière de sécurité et à fortiori la modification du comportement des employés et des utilisateurs.

Consciente de cette problématique, la DGSSI a mis en place un mécanisme de contrôle permettant d'inciter les différentes parties prenantes à mettre en place des programmes de sensibilisation au profit de leur personnel, notamment à travers les audits de conformité à la DNSSI. Par ailleurs, la DGSSI veille depuis 2013, à l'organisation de séminaires d'information et de sensibilisation sur la cybersécurité. Ces séminaires, qui mettent à contribution des experts nationaux et étrangers, traitent chaque année des thématiques d'actualité.

Focus

sur le Master Spécialisé en Cybersécurité

Cette formation, étalée sur quatre semestres, est ouverte aux ingénieurs et assimilés, relevant des organismes publics, des infrastructures d'importance vitale, ainsi que des organes de sécurité et de défense.
Dans le cadre de son ouverture sur son environnement régional, la DGSSI offre des places de formation au profit de certains ingénieurs et cadres de certains pays africains.
Le Master met un accent particulier sur les technologies en cours d'émergence et intègre des modules permettant la préparation à des certifications internationales, touchant aux différents aspects de la sécurité des systèmes d'information. Le diplôme délivré par l'Institut National des Postes et Télécommunications (INPT) est un Master spécialisé en cybersécurité, accrédité par le Ministère de l'Enseignement Supérieur.
Ce master répond à l'objectif, affiché depuis 2015, date de la première édition, de doter les organismes de l'Etat de ressources humaines qualifiées capables de relever les défis de cybersécurité au sein de ces organismes. Avec la 7ème édition du master, la DGSSI a pu former à ce jour, plus de 300 cadres relevant de l'ensemble des organismes de l'Etat et des Infrastructures d'Importance Vitale publiques et privées.
La DGSSI, estime que l'atteinte de cet objectif devra passer inéluctablement par l'affectation desdits cadres dans des fonctions liées à la cybersécurité, notamment celles exigées par la nouvelle loi sur la cybersécurité (RSSI, Auditeur...etc).
Par ailleurs, le programme du master est revu régulièrement ,afin d'intégrer des modules traitant des dernières évolutions techniques et technologiques en matière de sécurité des systèmes d'information. Ce programme comprend aussi la réalisation d'exercices «cyber», dont le scénario est adapté au contenu de chaque semestre.
L'objectif pédagogique principal de ces exercices est de mettre les stagiaires du Master dans une situation professionnelle réaliste, simulant des attaques cybernétiques, ainsi que les parades adoptées pour s'en défendre.

Toujours dans le cadre de la sensibilisation, et en plus des notes d'informations diffusées auprès des RSSI, la DGSSI élabore et publie régulièrement au niveau de son site institutionnel ***(www.dgssi.gov.ma)*** des guides de bonnes pratiques et de sensibilisation sur des thématiques de cybersécurité. Parmi les objectifs de ces guides figure le développement des réflexes de base « dits d'hygiène » relatifs à la protection des actifs informationnels et des systèmes d'information chez les usagers.

POLICE

La lutte contre les cybermenaces est tributaire d'une coopération nationale et internationale étroite et coordonnée, comment est positionnée la DGSSI dans ce domaine?

En effet, la protection du cyberespace national nécessite de s'appuyer sur un large tissu de coopération nationale et internationale.

Au niveau national, la DGSSI tisse des liens de coopération avec le secteur public et privé, ainsi que les universités, afin de créer les synergies nécessaires au développement d'une compréhension commune des risques cybernétiques au niveau national et de créer les conditions pour le développement de solutions souveraines en matière de cybersécurité et de services numériques.

C'est ainsi que depuis 2019, le plan d'action de la DGSSI a intégré le programme d'homologation des prestataires d'audit de la sécurité des systèmes d'information. L'objectif de ce programme est de développer au Maroc des bureaux d'étude exerçant leur activité sous juridiction marocaine, pour assurer des audits de sécurité des systèmes d'information sensibles des infrastructures d'importance vitale. Le marché des audits au Maroc a été boosté depuis 2016 par la diffusion du décret relatif à la protection des systèmes d'information sensibles des infrastructures d'importance vitale et ce marché sera boosté davantage avec la loi 05-20 sur la cybersécurité. Cette loi intègre également la réglementation d'autres services qui auront certainement un impact favorable sur la cybersécurité au Maroc, à travers un apport complémentaire aux missions assurées par la DGSSI, notamment par la mise en place de services de CERT privés, des fournisseurs de SOC, des fournisseurs de services numériques (Datacenters, Cloud national, Cloud souverain, etc.)

Tout le chalenge serait de créer le marché national qui pourra favoriser l'éclosion de ce type de service mis en place par des PME marocaines.

Les services pertinents que la DGSSI souhaite voir se développer au niveau national :

- La mise en place de CERTs privés et CERTs sectoriels (Banques, Assurances, industries, etc.) ;
- L'émergence de solutions Cloud « SaaS » nationales;
- Le développement de solutions de sécurité (Threat intelligence, Cryptologie, Firewalling, etc.);
- Les services de confiance.

La DGSSI développe également des collaborations et des partenariats avec les universités pour le renforcement des compétences nationales en matière de cybersécurité. Des programmes de formation riches et diversifiés ont été mis en place au profit de son personnel, mais également à destination du personnel de l'ensemble des départements ministériels, des organismes publics et des infrastructures d'importance vitale publiques et privées. C'est ainsi, que dans le cadre de la coopération avec l'Agence Nationale de Réglementation

La formation et les exercices de simulation organisés à l'échelon national, pour le renforcement des capacités nationales en cybersécurité, identifier les bonnes pratiques et renforcer la coordination.

Plateforme de simulation «Cyber Range»

des Télécommunications «ANRT», un Master spécialisé en cybersécurité a été mis en place depuis 2015, au niveau de l'Institut National des Postes et Télécommunications « INPT».

Un effort particulier devra en outre être fait pour déployer ce type de programme de formation dans d'autres universités scientifiques et techniques, ainsi que dans certaines écoles d'ingénieurs où ce type de formation est quasi inexistant dans les cursus de formation. Il serait aussi opportun d'intégrer des modules de formation «Cyber» dans les cursus des écoles primaires et secondaires (Hygiène cybersécurité).

Au niveau international, les populations du Monde profitent largement des vertus d'Internet, mais subissent aussi le fléau de la menace cybernétique. Une action malveillante à l'autre bout du monde peut rapidement avoir un impact planétaire. De ce fait, la protection est certes d'abord une question de souveraineté, elle est, en raison des interdépendances des réseaux et des systèmes, une affaire multilatérale. La menace est transnationale, la réponse devra être internationale.

Dans ce contexte, la coopération internationale s'impose comme un levier incontournable pour faire face à la menace cybernétique. Elle constitue un garant de la sécurité et la stabilité et un moyen d'échange et de partage de l'information et des bonnes pratiques entre les Etats.

La coopération internationale constitue également un moyen idoine de transfert de compétences permettant aux pays en développement de profiter de l'expertise des pays avancés pour développer leurs capacités dans le domaine de la cybersécurité.

Consciente de l'importance de cet aspect, la DGSSI a fait de la coopération internationale un axe majeur de sa stratégie de cybersécurité, tant sur le plan bilatéral que multilatéral. La DGSSI est ainsi, un membre actif de nombreuses structures et organisations internationales, dont le Groupe d'Experts Gouvernementaux de la Cybersécurité créé par l'ONU (GGE), dont la mission principale consiste en l'élaboration de normes internationalement acceptées pour instaurer un comportement responsable des Etats dans le cyberespace, le Forum of incident Response and Security Teams (FIRST) qui est une organisation mondiale regroupant la majorité des CERTs publics et privés, dont l'adhésion permet, outre la veille sur les tendances en matière de cybersécurité, la réponse efficace aux incidents de sécurité en donnant accès aux meilleures pratiques, aux outils et à une communication fiable avec les équipes membres, et le Global Forum on Cyber Expertise (GFCE), une communauté multipartite regroupant des gouvernements, des organisations internationales, des organisations non gouvernementales, la société civile, des entreprises privées, la communauté technique et le monde universitaire, qui vise à renforcer les capacités et l'expertise en matière de cybernétique au niveau mondial.

Sur le plan bilatéral, la DGSSI a tissé des relations de coopération avec les entités similaires des pays leaders dans le domaine de la cybersécurité notamment, la France, les Etats-Unis, l'Espagne, la Corée du Sud, l'Inde et la Malaisie. La DGSSI coopère également avec SANS « Escal Institute of Advanced Technolgy », une compagnie américaine spécialisée dans la sécurité de l'information et la formation sur la cybersécurité, pour le renforcement des compétences et l'échange de bonnes pratiques et d'expertise.

Aussi, La DGSSI a entretenu courant 2020 des échanges avec le Royaume Uni pour la mise en place d'un plan d'action de coopération en matière de cybersécurité entre la DGSSI et le NCSC (National Cyber Security Center). Ces actions de coopération visent notamment à supporter la DGSSI dans sa démarche de mise à niveau de la stratégie nationale de cybersécurité et la définition des programmes d'implémentation qui s'en suivraient. Elles visent aussi à renforcer les capacités nationales à travers le partage d'expérience, la formation et l'assistance. Le processus de développement d'une stratégie nationale de cybersécurité étant souvent facilité par la réalisation (ou la révision) d'une évaluation nationale de la maturité et des risques de cybersécurité, il a été convenu de placer ces deux projets en première priorité.

POLICE

Qu'en est-il du volet recherche et développement ?

La recherche et développement constitue l'un des principaux axes de la stratégie nationale de cybersécurité. De ce fait la DGSSI intègre en son sein une structure de recherche qui comporte plusieurs équipes multidisciplinaires. Ces équipes se focalisent principalement sur des activités de recherche appliquée dans des domaines ayant trait aux solutions de sécurité où la confiance requiert une importance capitale. Les problématiques traitées, relèvent de domaines aussi variés que la cryptographie, la cryptanalyse, la détection des intrusions ou encore la sécurité des échanges électroniques.

La promotion de la recherche dans ces domaines a pour but d'apporter des solutions aux problématiques de sécurité auxquels les parties prenantes sont confrontées au quotidien. Ces recherches tirent profit du retour d'expérience des équipes de la DGSSI et se basent sur des travaux de recherche réalisés en collaboration avec des professeurs universitaires et laboratoires nationaux. L'intérêt est de disposer de solutions basées sur des technologies hardware et software maîtrisées, évolutives et répondant à des cahiers de charge spécifiques ■

© 2021 DGSN

M. Omar SEGHROUCHNI

Président de la Commission Nationale de contrôle de la protection des Données à caractère Personnel

La protection des données personnelles..*un préalable pour un digital sûr et responsable*

Dans un écosystème numérique en expansion, la protection des données personnelles constitue un préalable stratégique et un prérequis fondamental, qui prenne en compte le respect de la vie privée. Dans un monde digitalisé où des données personnelles envahissent la toile, la donnée devient un actif stratégique et sa protection devient alors, gage de confiance, pour une transformation digitale réussie et responsable.

La Protection des données personnelles et de la vie privée est un droit constitutionnel consacré par les articles 24 et 27 de la Constitution de 2011. En outre, le Maroc, soucieux de protéger les citoyens, a mis en place un cadre institutionnel et réglementaire à même de consolider et de renforcer la protection des données personnelles. C'est ainsi que la Loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel fut promulguée en 2008, par laquelle a été instituée la Commission Nationale de contrôle de la protection des Données à caractère Personnel, en tant qu'autorité nationale, qui garantit la conformité de tout traitement des données personnelles avec le cadre réglementaire, et qu'il ne porte aucune atteinte à la vie privée, aux libertés et droits fondamentaux de l'Homme.

La Revue de Police a été accueillie au siège de la Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP), par son **Président M. Omar SEGHROUCHNI**, *qui a bien voulu répondre à nos questions, afin d'éclairer le lectorat sur les missions de cette commission stratégique et ses réalisations, pour consolider la confiance et accompagner la transformation digitale engagée par notre pays.*

La CNDP est l'autorité, qui dans une position de tiers de confiance doit permettre, d'une part, de rassurer le citoyen sur le fait que ses données à caractère personnel ne sont pas traitées de façon illicite

Article 24 : *« Toute personne a droit à la protection de sa vie privée »*

Article 27 : *«... Le droit à l'information ne peut être limité que par la loi, dans le but d'assurer la protection de tout ce qui concerne la défense nationale, la sûreté intérieure et extérieure de l'Etat, ainsi que la vie privée des personnes, de prévenir l'atteinte aux droits et libertés énoncés dans la présente Constitution ...»*

POLICE

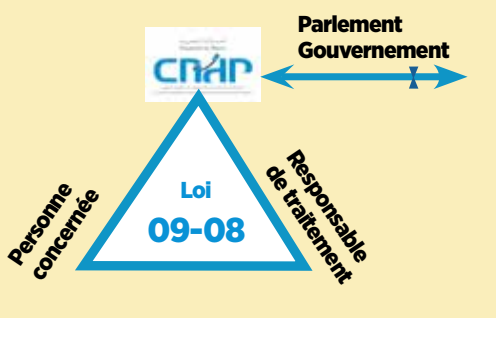
Quelles sont les missions de la CNDP ?

Dans notre pays, le respect de vie privée est garanti par l'article 24 de la Constitution, qui stipule que *« Toute personne a droit à la protection de sa vie privée. ... »*, et la protection des données à caractère personnel est portée la loi 09-08, dont l'application et la mise en œuvre sont assurées par la Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP), instituée en vertu de celle loi et installée en 2010.

Les missions et le fonctionnement de la CNDP sont régies par trois textes réglementaires. Il s'agit de :

- Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (BO n° 5714 du 05/03/2009);
- Décret n° 2-09-165 du 21 mai 2009 pris pour l'application de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (BO n° 5744 du 18/06/2009) ;
- Décision du 1er Ministre n°3-33-11 approuvant le règlement intérieur de la CNDP du 28 mars 2011 (BO n° 5932 du 07/04/2011).

Pour comprendre les missions de la CNDP, il faut analyser les interactions entre les 3 sommets d'un triangle. La base du triangle est constituée par la relation entre, d'une part, le citoyen auprès de qui on collecte des données



à caractère personnel et, d'autre part, l'entreprise, l'administration, l'association, etc... qui collectent ces données en vue d'en faire une utilisation particulière. Dans ce cas, on dit que la personne concernée (le citoyen) confie ses données à caractère personnel à un responsable de traitement (entreprise, administration, association, etc...) en vue d'une finalité particulière.

Cette relation ou ce contrat, entre la personne concernée et le responsable du traitement, doit répondre à certaines conditions fixées par la loi 09-08. Et l'autorité de contrôle, la CNDP, installée en 2010, a pour mission, entre autres, de vérifier que ce contrat respecte la loi.

La CNDP est l'autorité, qui dans une position de tiers de confiance doit permettre, d'une part, de rassurer le citoyen sur le fait que ses données à caractère personnel ne sont pas traitées de façon illicite, et d'autre part d'accompagner le responsable de traitement pour l'orienter vers les bonnes pratiques qui lui permettront d'honorer la confiance de la personne concernée.

La CNDP reçoit les plaintes de toute personne concernée estimant être lésée par la publication d'un traitement de données à caractère personnel. En effet, la Commission est dotée des pouvoirs d'investigation, d'enquête et de sanction. Elle mène dans ce sens, une mission permanente d'information du public et des personnes concernées sur les droits et obligations.

Par ailleurs, la CNDP donne son avis au gouvernement et au parlement sur les projets ou propositions de lois ou projets de règlements relatifs au traitement de données à caractère personnel dont elle est saisie.

POLICE

Qu'entend-on par protection de données personnelles ?

La loi 09-08 définit les données à caractère personnel comme étant toute information, de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image,

Pour vivre digital, il faut respirer protection des données à caractère personnel

concernant une personne physique identifiée ou identifiable.

Parmi ces données à caractère personnel, vous trouvez les données sensibles que la loi 09-08 définit comme pouvant révéler l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale de la personne concernée ou qui sont relatives à sa santé y compris ses données génétiques.

Vous savez, de nos jours, toutes les traces numériques que vous laissez sur Internet (habitudes de consommation, habitudes de navigation, habitudes de lecture, habitudes de conversation, ...), sont également des données à caractère personnel dès lors que l'on sait remonter aux personnes concernées. C'est ce qu'on appelle les données comportementales. C'est l'enjeu stratégique des années à venir.

Quelle place occupe la protection des données personnelles dans le schéma national de cybersécurité ?

Je dis souvent que *« Pour vivre digital, il faut respirer protection des données à caractère personnel»*. Nous disons aussi que *«Pour vivre digital, il faut respirer confiance numérique »*.

La place des données à caractère personnel est centrale. La protection des données à caractère personnel contribue à la confiance numérique. Et sans celle-ci, tout développement du digital sera incomplet.

Quels sont les défis et les enjeux inhérents à la protection des données personnelles ?

Les défis et enjeux inhérents à la protection des données à caractère personnel sont à la fois sociétaux et économiques.

Collecter des données à caractère personnel en vue d'être en mesure de fournir un service est un acte naturel... Cela n'est ni nouveau, ni lié au digital... Pour prendre un rendez-vous médical, il faut bien donner votre nom, votre prénom et peut-être d'autres informations. Ceci s'appelle une collecte de données à caractère personnel et cela permettra d'assurer un traitement : celui de la planification et de l'organisation du rendez-vous médical.

Ce traitement se fera manuellement ou de façon automatique, grâce au digital par exemple. La loi 09-08 s'applique aux deux.

Et c'est le médecin, le cabinet médical, la clinique ou la structure hospitalière que vous visitez qui est responsable du traitement des données à caractère personnel que vous lui avez communiquées.

Il y a des situations pour lesquelles la collecte des données à caractère personnel n'est pas nécessaire; ou plus précisément, n'était pas demandée : par exemple, avant la pandémie, pour acheter un ticket de bus, un billet de cinéma, un billet de théâtre, etc... Par contre, pour prendre un avion, ou pour s'inscrire à une formation, il faut fournir des données à caractère personnel.

Ceci existait bien avant l'ère du digital et la protection réglementée par la loi 09-08 qui concerne les données à caractère personnel sur tout type de support : informatique, papier, etc...

Ainsi, nous pouvons dire qu'il y a des situations où la collecte des données à caractère personnel est entendue, et d'autres où cela n'est pas habituel.

Mais les habitudes, et surtout les contextes, peuvent changer... De nouveaux usages sont créés. Par le passé, monter dans un autocar, ou dans un train, ne nécessitait pas forcément de décliner son identité. Mais pouvait nécessiter de décliner d'autres données à caractère personnel, son âge, sa situation d'handicap, si vous êtes retraité, etc... Si vous payez en espèce, aucun lien ne peut être fait avec votre personne. Si vous payez en carte bancaire ou par un moyen traçable, la relation avec votre personne peut être faite.

Nous dirions « Et alors ? » Si la relation avec votre personne est faite ? Quel est le problème ? Si cela permet de préserver vos droits, par exemple, éviter que quelqu'un se fasse rembourser à votre place, ou si cela permet de réduire la fraude, il n'est pas

raisonnable d'exprimer sa réticence. Cependant, si cela sert à autre chose ... par exemple, qu'une personne malintentionnée apprenne que vous avez voyagé et qu'elle organise un cambriolage, cela peut être problématique.

Donc, la question à discuter n'est pas le fait de collecter... mais le fait de protéger ce qui a été collecté.

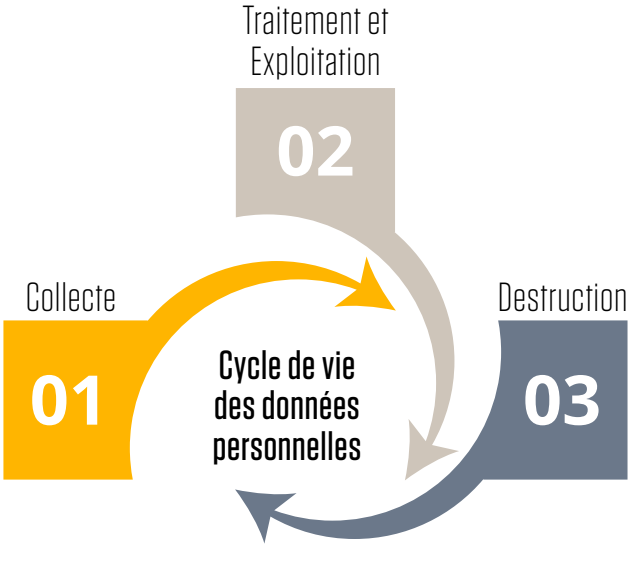
Pour cela, il faut respecter quelques règles de bon sens. Un traitement de données à caractère personnel, se fait en trois étapes:

- La collecte;
- Le traitement ou l'exploitation;
- La destruction.

Il faut donc:

- Veiller à collecter juste le minimum de ce qui est nécessaire pour assurer l'objectif, la finalité. Ce qui permet de réduire les risques d'utiliser ces informations à mauvais escient par la suite. Moins nous en avons, moins nous risquons d'en perdre ou de mal nous en servir.
- S'engager à ne pas s'en servir pour autre chose que ce que vous avez pu annoncer.
- Veiller à les protéger et à empêcher que des intrus ou des personnes tierces accèdent aux données de façon malencontreuse.
- Détruire les données à caractère personnel dès lors qu'on en a plus besoin. Cette durée de conservation doit être définie et partagée au moment de la collecte.

Il arrive à certains de penser que la base légale de la collecte est le seul consentement. Et que toutes les autres raisons sont dérogatoires : intérêt légitime, mission d'intérêt public, etc. Et pourtant, ce n'est pas le cas. Il faut comprendre qu'il existe plusieurs bases légales... plusieurs licéités. Elles sont aussi acceptables les unes que les autres. Le plus important est que la définition de cette base légale reste en cohérence avec les autres dispositifs de protection garantis par la loi.



> *Le Maroc a ratifié la Convention 108, relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe*

Ce n'est pas parce que nous sommes en position de collecter certaines données à caractère personnel (pour sauver la vie d'un patient, pour déployer un dispositif fiscal, pour vendre un abonnement, etc.), que nous pouvons nous autoriser à les gérer sans règles.

D'où l'importance de veiller au respect des bonnes pratiques, après la collecte. Si ces règles ne sont pas appliquées et contrôlées après la collecte, c'est comme si vous livriez vos données à l'inconnu. Il devient vite incohérent qu'une entreprise collecte vos données, en toute conformité, et qu'elle les livre à une autre entreprise, sur le territoire national ou à l'étranger, qui elle, ne respecte pas les règles. Il ne s'agit que de bon sens. Tout le flux de circulation des données doit rester protégé. Sinon, nous aurons pratiqué le fameux «wayloun lil al moussalin... ». Le respect de la protection des données à caractère personnel ne s'arrête pas au droit de les collecter.

Une fois que l'on a compris tous ces éléments, on comprend mieux les défis qui restent à relever. Là aussi, nous avons un triangle, dont les 3 sommets sont le citoyen, l'économie et l'Etat.

- Le citoyen et sa vie privée doivent être protégés.
- L'économie du pays, en vue de s'insérer dans la chaine de valeur internationale, au niveau du digital, doit utiliser les données à caractère personnel de la meilleure façon, ce qui lui permettra de gérer des partenariats et sous-traitances avec des donneurs d'ordre régionaux ou internationaux qui, pour respecter leurs propres réglementations, ne peuvent travailler qu'avec des économies qui respectent les données à caractère personnel.
- L'Etat doit veiller à ce que le patrimoine national, en termes de données à caractère personnel, ne soit ni dilapidé, ni utilisé à des fins incompatibles avec les intérêts de la collectivité.

POLICE

Est-ce que la cadre règlementaire national permet d'appréhender les nouveaux défis technologiques, comme les Deep fakes, les objets connectés, l'Intelligence Artificielle, etc.?

Le cadre réglementaire est en train d'être mis en conformité avec les standards internationaux. L'année 2022 va être une année charnière pour une mise à jour pour un déploiement en 2023. Concernant la protection des données à caractère personnel, le Maroc a ratifié la Convention 108, relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe. Il se prépare à intégrer la version modernisée de cette Convention, dite Convention 108 plus . Le Maroc est également en processus d'adoption de la Convention de

Malabo de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel

Ce qu'il faut bien comprendre c'est que les données à caractère personnel ne sont pas protégées en empêchant leur utilisation, mais en réglementant celle-ci. La loi 09-08 porte sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Il s'agit de bien cadrer les traitements. Les algorithmes et l'IA sont des traitements particuliers. La loi 09-08 permet déjà de les apprécier. Mais, il faudra aller plus loin lors de la refonte de la loi en cours.

Les objets connectés vont générer une foultitude énorme de nouvelles données, dont beaucoup seront à caractère personnel. Il s'agira de traiter les problématiques de proportionnalité (ne pas collecter plus que nécessaire) et les problématiques de loyauté et de conformité des traitements de ces données connectées.

Les fakes news sont de différents types. Les deepfakes sont, en général, «construits » à partir de données à caractère personnel. Leur appréciation entre dans le champ de la loi 09-08.

POLICE

Comment la CNDP accompagne les différents acteurs pour assurer une protection optimale de ces données ?

La CNDP a adopté une stratégie multidimensionnelle basée sur plusieurs actions :

- *Des actions organisationnelles pour réduire les délais d'instructions, via la* réorganisation interne et le déploiement d'une culture agile, la mise en place d'un front-office, le développement d'une culture de services orientée entreprises, administrations et citoyens.
- *Le déploiement d'une plate-forme de notifications dématérialisées.*
- *La préparation des modalités d'un contrôle a posteriori.*
- *Une sensibilisation territoriale allant jusqu'à l'encouragement de formations spécialisées de DPO (Data Protection Officer).*
- *Un travail pour organiser les relations avec les mandataires et améliorer l'efficacité des instructions aussi bien des dossiers de notifications que celles des plaintes.*

> *La « Privacy by Design » est, de ce fait, une pratique de bonne gouvernance, qui permet de rationaliser les délais finaux de conception et d'optimiser le time-to-market.*

POLICE

Est-ce que le concept du « privacy by design », est appliqué au Maroc?

La « Privacy by Design » est la prise en compte de la vie privée dès la conception des systèmes. Mais, nous citerons, également, l' «Architecture d'Entreprise» qui se hisse au statut de discipline de conception favorisant les études d'impact et l'exploitation des systèmes. Ces deux méthodologies nous aident à mieux identifier les manipulations de données à caractère personnel, et, de ce fait, à mieux prévoir et contrôler leur protection.

Le principe de Privacy by Design a été décrit, au début des années 1990, principalement par Ann Cavoukian, qui a été, par ailleurs, présidente de l'autorité de protection des données à caractère personnel au sein de la province de l'Ontario, au Canada. Ce principe est aujourd'hui repris dans l'essentiel des réglementations internationales.

Il s'agit de penser la vie privée en amont et ne pas la considérer comme la dernière roue du carrosse. Il faut la traiter au moment des réflexions en amont sur les projets, sur les lois, et pas comme une simple formalité à faire valider par une quelconque chambre d'enregistrement, une fois que tout est prêt pour le déploiement.

La vie privée n'est pas la cerise sur le gâteau, mais un des ingrédients de celui-ci, qui le rendra comestible ou indigeste.

Souvent, à la CNDP, nous recevons des dossiers de notification, pour lesquels il faut donner une réponse quelques jours après. Alors que, souvent, les projets concernés ont été initiés plusieurs mois avant.

Le fait de ne pas avoir eu recours à la «Privacy by Design » peut poser plusieurs problèmes. D'abord, l'entreprise ou le responsable de traitement peut se trouver dans la situation où il a fait des choix, défini des architectures et sélectionné des sous-traitants qui parfois -choix, architectures ou sous-traitants- ne sont pas en complète conformité avec la loi 09-08. Dans ces cas, une fois les choix effectués, il devient compliqué de faire marche arrière et de défaire ce qui a été construit.

Si les échanges avec la CNDP avaient été mis en place plus tôt, tout le monde y aurait trouvé un bénéfice :

- D'une part, le responsable du traitement aura été alerté assez tôt, avant ses investissements divers, et il aurait pu faire ses choix en bénéficiant d'un meilleur éclairage sur les problématiques liées à la vie privée.
- D'autre part, l'autorité de contrôle, la CNDP, aura eu plus de temps pour instruire le dossier et tout le

monde aura contribué à éviter de faire que la conformité ne se retrouve sur le chemin critique. La conformité est un ingrédient qui doit renforcer la qualité des projets.

La « Privacy by Design » est, de ce fait, une pratique de bonne gouvernance, qui permet de rationaliser les délais finaux de conception et d'optimiser le time-to-market.

Un des autres intérêts de la *«Privacy by Design»* est qu'elle favorise, auprès de l'entreprise, une réflexion au niveau de ce que les experts appellent l'*«Entreprise Architecture»*.

L'Architecture d'Entreprise est une méthodologie, de plus en plus utilisée depuis une vingtaine d'années, dont les premiers concepts ont émergé, dans les années 1970, chez IBM, puis, pendant les années 1980, avec le célèbre framework de Zachmann. Mais, beaucoup d'eau a coulé sous les ponts depuis. Les concepts et les outils ont évolué. Cette façon de voir permet de traiter au sein du même modèle plusieurs niveaux : la vision stratégique, la vision processus et organisation, la vision applicative ainsi que les différents niveaux d'infrastructure technique (informatiques ou autres). Ces concepts s'appliquent à tout type de projet.

La CNDP travaille actuellement pour déployer, de façon innovante, ce type d'approche, afin de simplifier et rationaliser l'instruction des dossiers de notification.

Cette méthodologie permettra de renforcer les approches de contrôle. Comme déjà évoqué en d'autres circonstances, la CNDP est une commission de contrôle, comme son intitulé le précise. Les opérations de contrôle, pour être bénéfiques, doivent s'aligner à l'intelligence de conception des systèmes, des architectures et des solutions. Aussi, il devient important de bien comprendre l'agencement pouvant exister entre les objectifs stratégiques, l'organisation humaine mise en place, les processus déployés, les traitements définis, les applications retenues et les infrastructures qui portent tous ces éléments.

Vous l'aurez compris, le respect de la loi 09-08 n'est pas qu'une simple question de formulaires... de nouveaux métiers sont en émergence. Un écosystème est à encourager et à favoriser. Les prochaines semaines et prochains mois renforceront ce propos, en particulier, suite à l'accélération que nous vivons tous, en cette période de pandémie.

POLICE

Quels sont les projets futurs de la CNDP ?

Nos projets futurs sont un : Contribuer humblement à faire de notre pays un exemple de respect de la protection des données à caractère personnel et de la vie privée. Pourquoi ? La réponse est simple: pour que sa position géographique et historique de carrefour entre plusieurs mondes soit stratégiquement confortée, dans ce nouveau monde, par une position de hub digital. Sans respect de la protection des données à caractère personnel, les flux divers et variés risquent de se détourner de notre pays.

Tout le reste en découle :

- La mise en place d'un contrôle a posteriori pour alléger les procédures de conformité et encourager le déploiement territorial de la conformité.
- L'accompagnement pour le développement de briques de confiance qui doivent peupler le digital national : visio-conférence, messagerie, datacenters, tiers de confiance national pour l'authentification...
- Le déploiement des programmes DATA-TIKA initiés par la CNDP en Juillet 2020.
- Le renforcement de notre positionnement à l'international.

La CNDP assure le Secrétariat Permanent du Réseau Africain des Autorités de Protection des Données Personnelles.

La CNDP a été élue en Octobre 2021 parmi les 8 membres de la GPA (Global Privacy Assembly) qui constitue l'organisation internationale regroupant les autorités de protection des données au niveau mondial.

> *Le citoyen doit éviter de communiquer ses données à caractère personnel dans un contexte non conforme*

POLICE

Quels conseils donneriez-vous à nos lecteurs pour renforcer la sécurité de leurs données personnelles dans le cyberespace?

En fait, nous devons réfléchir tous ensemble à ce que nous voulons pour notre pays. Il nous faut un digital responsable. Comment créer une véritable stratégie d'où pourra découler une hygiène de vie pour le digital. Comment éviter que le digital ne devienne un véritable stupéfiant, une drogue que nous utilisons sans discernement.

Aujourd'hui, certaines plateformes internationales arrivent à capter l'intérêt des citoyens, en direct, et s'en servent pour ne pas appliquer les lois nationales.

Le citoyen doit éviter de communiquer ses données à caractère personnel dans un contexte non conforme. C'est comme pour son argent. Tous les établissements financiers sont conformes. Il faut que les dépositaires de nos données à caractère personnel soient conformes. Il ne faut pas qu'il y ait de « blanchiment de données à caractère personnel ». Et c'est la prise de conscience des citoyens qui aidera aux usages responsables.

Le citoyen ne doit pas contribuer à la diffusion des fakes news, en se laissant aller à cette maladie contemporaine que je qualifie de « transférite ». Parfois, l'information est transférée sans en avoir pris connaissance, sans avoir vérifié son fondement. Il faut éviter de contribuer aux effets néfastes d'une circulation illégitime des informations non vérifiées ■

LE SYSTÈME D'INFORMATION DE LA DGSN..

EXPERTISE, MATURITÉ ET RÉSILIENCE

La sécurité des systèmes d'information n'est pas une nouvelle donne à la DGSN. Elle a toujours constitué une priorité, et ce, il y a plus de 45 ans. En effet, la mise en place d'un système d'information « SI » à la DGSN date de 1976. Depuis, ce système ne cesse de se développer et d'évoluer, en apportant à chaque fois de nouvelles briques.

Dans sa version ancienne, l'architecture du « SI », était composée de serveurs et de terminaux spéciaux, dont l'accès était seulement permis à des personnes habilitées, via des logins et des mots de passe, avec une sécurité et traçabilité renforcées. En 1982, la DGSN disposait de son centre informatique, le premier en Afrique. La sécurité était toujours une priorité, comprenant la sécurité physique des locaux « critiques », la redondance de l'alimentation électrique, la mise en place de groupes électrogènes, etc.

Depuis, la DGSN n'a cessé de développer et de faire évoluer son SI, par l'acquisition d'une nouvelle plateforme informatique pour étendre son réseau, tout en renforçant les mesures de sécurité et de protection et en considérant la sécurité en amont, dans tout processus de développement. C'est ainsi qu'en 2008, la DGSN a mis en production de nouveaux systèmes, notamment pour la carte nationale d'identité. Depuis, la DGSN a poursuivi le développement et l'extension de son SI, en apportant de nouvelles briques à son Data Center, riche de plusieurs applications informatiques, pour faciliter le travail des policiers, mais également améliorer et simplifier les services rendus aux citoyens.

Le SI actuel de la DGSN est un SI mature, riche et diversifié, du système identitaire, applications métiers, messagerie électronique interne, aux systèmes ouverts sur Internet et d'interfaçage avec les partenaires, avec une sécurité qui reste toujours une priorité des plus fondamentales. Et quand on parle de sécurité, elle est appréhendée dans son sens le plus large, allant de la sécurité physique des installations et des sites, des accès logiques, des données, des échanges, des réseaux, à la continuité d'activité en cas d'incident. Un SI résistant, redondant et résilient.

Ce développement a été accompagné par un renforcement des compétences techniques de la DGSN, par le recrutement de profils pointus, des docteurs, des ingénieurs et des techniciens toutes disciplines confondues, auxquels est confiée la mission du développement, mais aussi celle de la protection et la sécurisation du patrimoine informationnel dont dispose la DGSN, au service de la sécurité de nos concitoyens.

Aujourd'hui, la DGSN est en pleine transformation numérique, pour plus de proximité avec les citoyens.

« Des ingénieurs et techniciens en réseaux, systèmes et sécurité travaillent de jour comme de nuit, pour veiller à la sécurité du SI de la DGSN »

Wafae OMARI

Chef du service «sécurité des systèmes», à la Direction du Système d'Information et de la Communication

La Revue de Police s'est entretenue avec une jeune femme, Ingénieur et Commissaire Divisionnaire, Chef du Service «sécurité des systèmes» à la Direction du Système d'Information et de la Communication, pour nous parler de la sécurité du SI de la DGSN et de la transformation digitale du service public policier.

Elle s'appelle Wafae OMARI, elle est Commissaire Divisionnaire et Ingénieur. Elle a intégré les rangs de la Sûreté Nationale en 2013, juste après l'obtention du diplôme d'Ingénieur d'Etat en réseaux et télécommunications décerné par l'Ecole Nationale des Sciences Appliquées « ENSA ». Elle a entamé sa carrière à la DGSN au service «sécurité» à la Direction du Système d'Information et de la Communication. La compétence et le sérieux de cette jeune femme lui ont valu, quelques années après, en 2017, sa nomination en tant que chef du service «sécurité des systèmes», relevant de la division déploiement et sécurité. Une responsabilité et non des moindres pour cette jeune cadre dévouée.

En quête continue d'amélioration de ses connaissances et compétences, cette jeune femme, en parallèle avec son travail, a obtenu un Master en Sécurité des Systèmes d'Information décerné par l'Institut National des Postes et Télécommunications en 2019. Elle est également titulaire de plusieurs certifications en cybersécurité reconnues à l'échelle internationale, dont notamment ISO 27005, risk manager, ISO 27001 lead auditor, GIAC Certfied Forensic Analyst (SANS), Certified Ethical Hacker (EC-Council), Certified SOC Analyst, etc.

Quelles sont les missions du service « sécurité des systèmes» que vous dirigez ?

Le service « sécurité des systèmes » relève de la Division «déploiement et sécurité» à la Direction du Système d'Information et de la Communication. Le service est composé d'ingénieurs et de techniciens en réseaux, systèmes et sécurité, qui travaillent de jour comme de nuit, pour veiller à la sécurité du SI de la DGSN.

Notre mission est de veiller à la mise en conformité du système d'information de la DGSN avec le cadre juridique national régissant la sécurité des systèmes d'information, ainsi que la politique de sécurité SI, de concert avec la Division de la sécurité des systèmes d'information relevant de l'Inspection Générale. Au sein du service, nous assurons également la réalisation d'études sur la structuration de l'architecture et du design, afin d'orienter les choix techniques de sécurité des systèmes d'information, l'administration et l'exploitation des solutions de sécurité, ainsi que la réalisation des tests et des audits de sécurité. Nous réalisons aussi le scan des vulnérabilités, nous assurons la veille et la supervision de la sécurité, ainsi que la sensibilisation des administrateurs aux enjeux de sécurité. Notre action intervient en amont, dans tout

le cycle d'un projet informatique, depuis la phase de conception, afin de statuer sur la solution de sécurité appropriée, et ce, après l'évaluation des risques potentiels. Notre action se poursuit lors de la phase déploiement du système, par la réalisation d'audits de sécurité et de tests d'intrusion, afin de vérifier si les correctifs formulés ont été bel et bien intégrés.

C'est loin d'être un nouveau concept à la DGSN, mais d'une philosophie de travail guidée par le souci de sécurité.

POLICE

Où en est la DGSN dans sa stratégie de digitalisation ?

Au vu de l'importance que revêt le chantier l'informatisation des métiers de la DGSN, de la dématérialisation et la numérisation des services publics en ligne offerts aux citoyens, ainsi que les défis sécuritaires qui en dérivent, les technologies de l'information sont placées d'une manière conséquente et opératoire au cœur même des plans stratégiques de la DGSN.

Dans le même sillage, la loi 55-19 relative à la simplification des procédures et des formalités administratives, a fixé un échéancier pour accomplir la dématérialisation des procédures et décisions administratives. Dès lors, la simplification des services offerts aux citoyens est en tête des prérequis vers cette transformation digitale.

Il faut savoir que la transformation numérique avec toutes les opportunités qu'elles apporte amène avec elle des risques grandissants et donc une obligation de se protéger contre les menaces émergentes. C'est pourquoi la sécurité est une composante essentielle pour une transformation digitale réussie.

Le SI de la DGSN est en constante évolution, afin d'accompagner et faciliter le travail des fonctionnaires de la DGSN dans l'accomplissement des missions qui leur incombent, mais aussi pour faciliter et améliorer les services offerts au grand public. En effet, l'informatisation et la simplification des processus métiers permet de gagner en efficacité et efficience et ajoute, au fur et à mesure de nouvelles composantes au SI de la DGSN, qui est de plus en plus complexe. Il s'agit des systèmes identitaires, des systèmes de gestion des postes frontières, des systèmes de gestion des arrondissements de police, des systèmes pour l'établissement des procès-verbaux des accidents de la circulation, etc. La liste s'agrandit de jour en jour.

Ces dernières années, la DGSN a lancé un ensemble de dispositifs d'interaction avec le grand public, qui ont pour but de simplifier, de dématérialiser les procédures administratives et garantir ainsi, la réception et le suivi des demandes en ligne. Il s'agit par exemple du portail dédiée aux concours d'accès aux rangs de la Sûreté Nationale ***« concours.dgsn.gov.ma»,*** permettant aux postulants aux concours de la DGSN de déposer leurs dossiers de candidature et de les suivre en ligne, et le portail ***«cnie.ma»***, qui permet aux citoyens de dématérialiser la demande et de suivre le processus d'établissement de leurs cartes nationales d'identité électronique, ainsi que la prise de rendez-vous en ligne.

Le portail de la CNIE.. un pas important vers la transformation numérique de la DGSN

> *Le SI de la DGSN est en constante évolution, afin d'accompagner et faciliter le travail des fonctionnaires de la DGSN dans l'accomplissement des missions qui leur incombent, mais aussi pour offrir des services au grand public*

Aussi, et poursuivant dans la lancée dynamique, la nouvelle génération de la carte nationale d'identité électronique lancée par la DGSN en août 2020, dispose d'éléments de sécurité renforcés, pour lutter contre la fraude et la criminalité organisée, en mettant en place un fondement, pour un climat de confiance numérique.

En effet, la nouvelle carte nationale d'identité électronique, en tant que document obligatoire, permettra de doter chaque citoyen d'une identité numérique dérivée de son identité régalienne, sécurisée moyennant des certificats numériques stockés dans la puce de la carte, qui lui permettront de s'identifier et de s'authentifier de manière fiable et sécurisée auprès des administrations publiques ou privées offrant des services aux citoyens, et cela selon les normes et standards des échanges de données numériques.

Lesdits certificats électroniques sont générés de manière sécurisée par le biais d'une plateforme de gestion des clés, dite PKI (Public Key Infrastructure) dédiée spécialement à cette fin, qui a été conçue en se basant sur les normes de sécurité nationales et internationales et en s'appuyant sur les dernières technologies en la matière.

A cet égard la DGSN, a mis des services en ligne basés sur la vérification de la carte nationale qui sont mis à la disposition des organismes publics et privés, pour renforcer l'aspect sécuritaire des opérations en ligne, ce qui positionnera la DGSN comme tiers de confiance national.

Qui dit digitalisation, dit cybersécurité. Comment la cybersécurité est-elle considérée et intégrée ?

La DGSN, bien consciente de l'importance que revêtent les systèmes mis à la disposition du grand public ou des organisations publiques et privées, a positionné la sécurité comme une partie intégrante des processus mis en place.

Dans cette même perspective, la cybersécurité est incontournable lors de la conception et la mise en place des systèmes de la DGSN, car le développement ou l'utilisation des nouvelles applications en ligne, et l'extension du périmètre réseau offrent plus de vecteurs d'attaques potentielles pour les hackers et en augmentent la surface. De plus, la crise pandémique a directement influencé l'espace «cyber» et a été un véritable catalyseur de diversification de la nature des attaques informatiques, chose qui a été constatée au Maroc, comme à l'étranger.

Le SI de la DGSN s'appuie sur une sécurité basée sur un système de protection en profondeur, constitué de plusieurs barrières ou couches de défense, dans lesquelles chaque couche pourrait être classée dans l'une des catégories suivantes:

- Des contrôles de sécurité physique déployés au niveau des locaux et composés de dispositifs de contrôle d'accès et une supervision continue en temps réel, via la vidéosurveillance, pour s'assurer que seules les personnes habilitées peuvent y accéder;
- Des contrôles techniques, pour protéger et préserver le système informatique contre les dénis de service, les accès non autorisés, le vol et l'altération des données. Un ensemble d'outils matériels et logiciels sont déployés à cette fin (antivirus, pare-feu, solutions de chiffrement, outils de détection et de supervision, etc.) ;
- Des contrôles administratifs, destinés au personnel de la DGSN, pour assurer le traitement, en toute sécurité de nos systèmes, ainsi que l'instauration d'une pratique efficace et efficiente de la sécurité. Il s'agit de la politique de sécurité des SI, des directives de sécurité, ainsi que des procédures d'administration et d'exploitation.

Une stratégie intégrée qui s'appuie sur des outils et des processus efficaces et sur une multitude de garde-fous.

Qu'en est-il de l'aspect légal adopté par la DGSN en matière de cybersécurité ?

L'un des objectifs principaux de la DGSN, lors de la conception et le traitement au niveau des services offerts aux citoyens, est de se conformer au cadre juridique national en vigueur.

Concernant la loi 05-20 relative à la cybersécurité, la DGSN est partie prenante au Comité Stratégique de la cybersécurité, institué en vertu de cette loi et qui est en charge de définir les orientations statégiques du Royaume en la matière. Dans cette même perspective, la DGSN a revu son organisation, pour la mise en application des dispositions de cette loi. Nous réalisons également les tests et les audits exigés en vertu de cette loi.

Il en est de même pour la loi 09-08, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, en vertu de laquelle la DGSN veille à obtenir l'autorisation de l'autorité compétente pour chaque système traitant ces données. En ce sens, la DGSN a obtenu l'autorisation pour le traitement des données personnelles auprès de la Commission Nationale de contrôle de la Protection des Données à caractère Personnel «CNDP», autorité nationale chargée du contrôle du respect des lois en matière de protection des données personnelles, aussi bien pour le portail de la Carte Nationale d'Identité Electronique, que celui des concours.

Quelles sont les démarches adoptées dans la pratique, pour assurer la cybersécurité ?

En matière de cybersécurité, l'approche adoptée par la DGSN s'appuie sur trois volets essentiels, la prévention, la détection et la réaction.

En matière de prévention, notre approche vise à assurer la résilience des différents services, par la mise en place de contrôles axés sur l'évaluation des risques, en adoptant une architecture technique permettant d'atteindre les objectifs de sécurité au niveau de quatre composantes clés, la disponibilité, l'intégrité, la confidentialité et la traçabilité, et ce, afin d'assurer une protection optimale contre toute menace.

Nous procédons également à l'évaluation de la

© 2021 DGSN

Le Centre de supervision de la sécurité du système d'information de la DGSN

fiabilité de nos systèmes et réseaux, via la réalisation de tests d'intrusion, d'audits de configuration des serveurs, des équipements réseaux et des codes sources, ainsi que des scans de vulnérabilité des systèmes, d'une manière régulière.

L'objectif ultime, étant de tester le niveau de sécurité des systèmes et d'identifier les failles potentielles, qui pourraient être exploitées par des personnes malintentionnées. Nous faisons également appel aux services de la Direction Générale de la Sécurité des Systèmes d'Information « DGSSI», qui compte parmi ses équipes, des profils pointus à l'échelle nationale, afin de réaliser des tests d'intrusion supplémentaires sur nos systèmes en ligne.

Cependant, et malgré toutes les mesures de sécurité mises en place, aucun système informatique au monde n'est infaillible. C'est pour cela, que la détection représente une action essentielle, pour ne pas dire cruciale, dans ce triptyque de la cybersécurité. D'où l'intérêt de mettre en place des systèmes de détection fiables et performants, et d'avoir du personnel de supervision, opérant 24h/24 et 7j/7. Ainsi, la détection s'appuie sur un suivi continu de l'état des systèmes, afin de réagir vite et de manière ordonnée en cas d'incident.

Enfin, la réaction à travers la mise en place d'un plan de réponse aux incidents, afin de s'assurer que le personnel de la DGSN est bien préparé et que les procédures nécessaires sont mises en places pour qualifier, délimiter, confiner et remédier à la situation.

POLICE

Vous avez précisé que la DGSN peut faire appel à la DGSSI pour réaliser des tests, qu'en est-il des partenariats et de la coopération avec les autres parties prenantes?

Dans un cyberespace de plus en plus vaste et complexe, faire face aux enjeux de la sécurité du numérique nécessite une coopération de toutes les parties prenantes. En effet, face aux enjeux sécuritaires en constante évolution, les moyens engagés par la DGSN sont soutenus par une synergie opérationnelle de coopération, aussi bien à l'échelle nationale qu'internationale. En plus de la DGSSI et d'autres partenaires nationaux, nous travaillons avec les organes d'application de la loi, soit au niveau bilatéral ou multilatéral.

Cette coopération concerne l'échange de connaissances sur les nouvelles technologies et techniques, les menaces émergentes, ainsi que le renforcement des capacités de détection et de réponses aux incidents, comme elle concerne le volet opérationnel, pour la gestion de crises cybernétiques.

> *L'un des objectifs principaux de la DGSN, lors de la conception et le traitement au niveau des services offerts aux citoyens, est de se conformer au cadre juridique national en vigueur*

POLICE

Le développement des compétences est une composante importante pour être à la hauteur des défis liés à la cybersécurité. Quels sont les efforts déployés par la DGSN dans ce volet ?

Bien consciente de l'importance que revêtent la formation et le développement des compétences et l'instauration d'une culture de cybersécurité, la DGSN ne cesse d'investir dans la formation continue et spécialisée de ses ingénieurs et techniciens en matière de sécurité. Ces formations concernent les dernières technologies en la matière, mais également des formations de pointe en matière de cybersécurité. Les cadres de la DGSN bénéficient également du Master spécialisé en cybersécurité co-organisé par la Direction Générale de la Sécurité des Systèmes d'Information et l'Agence Nationale de Réglementation des Télécommunications. Nos équipes techniques participent également à des exercices de simulation de cyberattaques au niveau national et international, pour développer les compétences techniques et les réflexes en matière de détection et de réponse à ces incidents. Nous participons également à des séminaires et formations à l'échelle nationale et internationale, pour l'échange d'expériences et de bonnes pratiques ■

DOSSIER

La Sécurité des Systèmes d'Information à la DGSN.. plus qu'une exigence, une philosophie de travail et une culture

La cybersécurité est un enjeu de sécurité nationale, intégrée désormais dans la stratégie nationale de sécurité de chaque Nation. En effet, l'évolution technologique fulgurante a induit une transformation radicale de notre façon de vivre, de consommer, de travailler, de nous divertir, etc. Une autre vie parallèle que nous menons à divers échelons de la société. On parle de nation numérique, une nation hyperconnectée avec l'explosion de l'usage d'Internet et des objets connectés, la dématérialisation des procédures administratives et une ouverture de plus en plus grande des SI aux services en ligne, facilitant ainsi notre quotidien.

Mais si le monde est à la portée d'un clic, la surface des cyberattaques augmente de plus en plus, et de nombreuses menaces planent sur la Nation, tant sur le plan individuel, que gouvernemental et économique. Le cyberespace est devenu alors un territoire envahi par des cyberdélinquants, des cybercriminels et des cyberterroristes, en quête de vulnérabilités, de cibles et un espace d'action où les frontières sont abolies, offrant de nombreuses opportunités à ces personnes malveillantes. Le flux important de données personnelles et sensibles, circulant dans le cyberespace est de plus en plus exposé à des menaces nouvelles et diverses. Les motivations peuvent être financières, d'intelligence économique, politique ou d'image. Et les exemples sont nombreux dans le monde.

Le risque « cyber » est devenu alors le nouveau risque à prendre en compte dans toute stratégie de sécurité, au même titre que les risques conventionnels. Un risque qui doit être évalué, apprécié et catégorisé, afin d'être en mesure de dimensionner les solutions de sécurité à adopter et d'être préparé à y faire face et à le traiter.

Au Maroc, à l'instar de plusieurs pays dans le monde qui a entamé sa transformation numérique, la cybersécurité est une priorité nationale, qui s'est traduite par un cadre de gouvernance intégré et cohérent, tant sur le plan juridique qu'institutionnel et partenarial, pour garantir la sécurité et la résilience des systèmes d'information stratégiques du Royaume et la DGSN en fait partie.

En application de ce cadre, les acteurs stratégiques sont tenus de mettre en conformité la sécurité de leurs systèmes d'information avec les référentiels de sécurité mis en place, afin de garantir une sécurité optimale et une résilience des SI, détecter et notifier rapidement à l'autorité nationale et aux services concernés tout incident ou attaque, participer à des exercices de cybersécurité et soumettre leurs SI à des contrôles et audits.

La DGSN, à l'instar d'autres organismes stratégiques, s'est organisée et a revu la gouvernance de la sécurité de son système d'information, pour la mettre en conformité avec les exigences légales, réglementaires et normatives. Une gouvernance transversale, pilotée par un comité stratégique, dont la supervision et le contrôle sont assurés par une structure dédiée exclusivement à la sécurité des systèmes d'information, la Division de la Sécurité des Systèmes d'Information « DSSI ». Une entité composée d'une équipe pluridisciplinaire hautement qualifiée, dont la mission principale est de veiller à l'application de la politique de sécurité des systèmes d'information de la DGSN et des normes en vigueur, et d'instaurer et consolider une culture de cybersécurité parmi le personnel de la DGSN.

La Revue de Police s'est entretenue avec le Contrôleur Général Mounir RAMI, chef de la Division de la Sécurité des Systèmes d'Information et lauréat de l'Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes à Rabat, pour décrypter le rôle de cette entité d'une importance vitale pour la DGSN.

Le Contrôleur Général
Mounir RAMI

est lauréat de l'Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes « ENSIAS » à Rabat en 2006. Après quatre années d'exercice dans le secteur privé, il intégra la DGSN en 2010 et exerça au sein du département informatique, puis au service de la gestion des infrastructures et clés cryptographiques à la Direction du Système d'Information et de la Communication. En 2013, il intégra la Division de la Sécurité des Systèmes d'Information après sa création en 2013 et son rattachement à l'Inspection Générale. En 2017, il fut désigné en tant que responsable du Service Etudes et Stratégie au sein de cette Division. Les compétences et le sérieux de ce jeune gradé et ingénieur d'Etat principal, lui ont valu sa nomination en tant que Chef de la Division de la Sécurité des Systèmes d'Information en 2019. Une entité stratégique qui veille sans relâche sur la sécurité et la résilience du SI de la DGSN et la consolidation d'une culture de cybersécurité parmi son personnel.


© 2021 DGSN

Quels sont les objectifs de la création de la Division de la Sécurité des systèmes d'Information «DSSI» ?

Dans un contexte d'accélération des technologies de l'information de la communication et leur appropriation par les différents acteurs de la société, tant les citoyens, que les institutions et les entreprises, la cybersécurité est devenue un enjeu stratégique et de souveraineté. Le Maroc, dans une approche globale et intégrée, a placé la sécurité des systèmes d'information des administrations et acteurs d'importance vitale au plan de ses priorités. C'est ainsi que le corpus réglementaire a été renforcé par la mise en place de la loi 05-20 relative à la cybersécurité, ainsi que des organes de gouvernance, notamment le Comité stratégique de la cybersécurité et l'autorité Nationale de cybersécurité.

Avant de répondre à la question, il me parait essentiel de revenir sur ce qu'est la cybersécurité. La Loi 05-20 sur la cybersécurité la définit comme étant « *l'ensemble des mesures, procédures, concepts de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies, permettant à un système d'information de résister à des événements issus du cyberespace, susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ce système offre ou qu'il rend accessibles* ».

La cybersécurité a donc pour but principal de soutenir les missions et les objectifs de l'organisation, en lui permettant de continuer à exister et à fonctionner correctement, face aux divers cyber-risques.

A la DGSN, la cybersécurité et la sécurité de l'information dans sa globalité, n'est pas un concept nouveau. Bien au contraire, c'est une composante essentielle, qui a toujours figuré parmi les orientations stratégiques de la DGSN, et ce, depuis sa création le 16 mai 1956. En effet, la DGSN n'a cessé de porter une attention particulière à la sécurisation et à la protection de son patrimoine informationnel, et ce, à travers la mise en place de plusieurs mesures de sécurité d'ordre organisationnel et technique, visant la préservation de ce patrimoine. D'ailleurs, la DGSN a été parmi les premières institutions nationales à mettre en place des mesures pour garantir la sécurité de l'information, constituant un référentiel en la matière. En effet, des circulaires et des notes directoriales datant des années 60, traitent du secret professionnel, de la sécurité physique et des accès, de l'accompagnement des visiteurs, des archives, des aspects techniques, etc. La sécurité de l'information à la DGSN, est une philosophie de travail et une culture, ancrées dans notre quotidien.

Cela dit, et dans un contexte de cybersécurité dynamique et diversifié, visant à faire face aux fortes montées des menaces cybernétiques au cours de ces dernières années, la DGSN a pris des mesures pour le renforcement de la protection de son système d'information, à travers la prévention, la détection, et la répression d'actes pouvant porter atteinte à la confidentialité, l'intégrité ou la disponibilité de ce système d'information. Mais également, la sensibilisation du personnel pour adopter les mesures de «cyber-hygiène», pour en faire un maillon fort et un vrai rempart contre toute atteinte à son patrimoine informationnel.

Au fil des années, la DGSN n'a cessé de s'approprier la technologie avec toutes ses nouveautés, pour mieux organiser et faciliter le travail de ses diverses entités, et cela est sans nul doute matérialisé par la création d'une Direction du Système d'Information et de la Communication. Une structure technique disposant de profils pointus et diversifiés, prenant en charge le SI de la DGSN, tant dans sa composante conceptuelle, sécuritaire que de contrôle et d'évaluation.

Afin d'institutionnaliser cet engagement, la DGSN a mis en place une stratégie globale et intégrée, visant la prévention, la détection et la réponse aux incidents pouvant compromettre la sécurité de son système d'information. Pour mettre en œuvre cette stratégie, des structures spécialisées dédiées à la sécurité de l'information, ont été créées et des ressources humaines qualifiées recrutées. C'est ainsi que la DGSN a fait le choix de séparer la fonction contrôle et évaluation de la sécurité des systèmes d'information du département technique, en créant la Division de la Sécurité des Systèmes d'Information (DSSI) et en la rattachant à l'Inspection Générale. Cette action, en plus de se conformer à la réglementation nationale en vigueur, vise à asseoir les bases d'une bonne gouvernance sécuritaire, en conférant à cette structure, l'indépendance nécessaire, afin d'exercer de manière efficace et efficiente, les missions de contrôle et d'évaluation de la sécurité des SI à la DGSN et de la promotion d'une culture de cybersécurité.

> *La sécurité de l'information à la DGSN, est une philosophie de travail et une culture, ancrées dans notre quotidien.*

POLICE

Quelles sont les missions de la Division de la Sécurité des Systèmes d'Information «DSSI»?

De manière globale, la « DSSI » est l'entité en charge de la mise en place du cadre de la gestion de la sécurité de l'information et de la mise en conformité du SI de la DGSN avec les exigences nationales en la matière. Ses missions vont de la mise en place du cadre global de la gestion de la sécurité de l'information, la mise en oeuvre de la politique de sécurité de l'information, l'analyse des risques pouvant peser sur le SI, la supervision de la sécurité, la sécurité physique et celle des postes de travail, la détection des menaces, à la réaction en cas d'incident, tout en assurant la coordination des actions menées en la matière avec les différentes parties prenantes de la DGSN, mais aussi avec l'autorité nationale en charge de la cybersécurité, à savoir la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI), ainsi que des partenaires externes.

Pour mener à bien ses missions, la DSSI comprend deux services :

- *Le service études et stratégie est chargé de l'élaboration des référentiels, notamment la politique de sécurité et les politiques connexes par domaine et veille sur leur mise en application;*
- *Le service exploitation et conseil, quant à lui est chargé du suivi, de la mise en place de procédures de gestion des incidents, la veille, de l'audit, ainsi que la formation et la sensibilisation.*

La « DSSI » est l'organe de contrôle organisationnel de la SSI. Elle est chargée de l'élaboration des référentiels en relation avec la SSI et veille à leur mise en oeuvre. Elle réalise des missions de contrôles et d'audits de sécurité, afin de vérifier principalement, la conformité et l'efficacité des mesures de sécurité mises en place, conformément aux dispositions de la politique de sécurité de l'information de la DGSN. Elle veille en amont, de concert avec la Direction du Système d'Information et de la Communication et les directions métiers, à l'intégration des exigences de sécurité dans tout projet se rapportant aux technologies de l'information, à la mise en place de dispositifs de supervision et de détection des événements de sécurité, et enfin à garantir une réponse efficace aux incidents liés à la sécurité de l'information.

D'autres missions sont dévolues à cette structure, à savoir la mise en place d'une approche de sécurité basée sur la gestion des risques cybernétiques, permettant le renforcement de la résilience du SI de la DGSN face aux divers risques encourus, la mise en place d'un cadre de gestion de la continuité des activités essentielles, tout en veillant à l'amélioration de leur résilience et enfin, veiller sur la conformité de la sécurité du SI de la DGSN avec l'ensemble des référentiels législatifs, réglementaires et normatifs en vigueur.

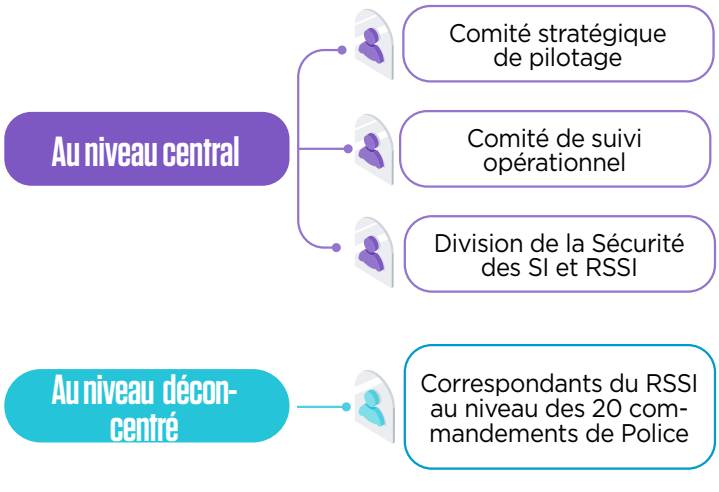
Quelles sont les principales mesures entreprises pour la mise en conformité du SI de la DGSN ?

Au lendemain de la création du Comité Stratégique de la Sécurité des SI et de l'adoption de la Directive Nationale de la Sécurité des SI «DNSSI», la DGSN a mis en place un comité stratégique, présidé par l'Inspecteur Général et composé des directeurs centraux et du chef de la Division de la sécurité des systèmes d'information.

Sa principale mission étant le pilotage du projet de mise en conformité du SI de la DGSN avec la Directive Nationale de la Sécurité des Systèmes d'Information «DNSSI», et la définition des orientations stratégiques en matière de sécurité de l'information de la DGSN, afin de les soumettre au Directeur Général de la Sûreté Nationale pour approbation.

« La DSSI réalise selon un plan annuel préétabli, des audits du SI tant au niveau central que déconcentré, établit les écarts par rapport à la DNSSI et propose les traitements à mettre en place pour y remédier. Elle assure le suivi permanent avec les différentes entités déconcentrées.

Structure organisationnelle de la SSI



Pour assurer le suivi opérationnel des différents chantiers de mise à niveau de la sécurité du SI de la DGSN, un comité de suivi de la sécurité des systèmes d'information a été institué. Il est présidé par le chef de la Division «DSSI» et constitué des représentants des différentes directions centrales de la DGSN.

Au niveau déconcentré, au sein de chaque commandement, a été institué le poste du correspondant du responsable de la sécurité de l'information. Mission dévolue aux responsables régionaux de la gestion d'urgence, qui font office de correspondants chargés de la SSI. Ces correspondants ont pour mission de sensibiliser le personnel relevant des services déconcentrés sur les directives de sécurité établies par la DGSN, d'alerter et de remonter à la DSSI, les incidents de sécurité pouvant impacter la sécurité de l'information de la DGSN.

La DSSI réalise selon un plan annuel préétabli, des audits de sécurité, tant au niveau central que déconcentré, établit les écarts par rapport à la DNSSI et propose les traitements à mettre en place pour y remédier. Elle assure le suivi permanent avec les différentes entités déconcentrées.

De par la réglementation, nous sommes tenus de transmettre à l'autorité nationale «DGSSI», un bilan annuel, qui traduit le taux de conformité du SI de la DGSN avec la Directive Nationale de la Sécurité des Systèmes d'Information.

Le travail n'est pas simple, il est tant technique qu'organisationnel et fait appel à une grande expertise et technicité, grâce aux compétences techniques de pointe dont dispose la DGSN, avec plusieurs ingénieurs et cadres en diverses disciplines, dont plusieurs ont été certifiés dans le domaine de la cybersécurité.

Quelle place occupe la DGSN dans le schéma national de la cybersécurité?

Depuis l'adoption de la stratégie nationale de la cybersécurité, la DGSN est une partie intégrée de cette stratégie et participe activement à tous les projets liés à la cybersécurité, en étroite collaboration avec les organes compétents à l'échelon national.

Avec l'adoption de la loi 05-20 relative à la cybersécurité, qui a institué les organes de gouvernance en la matière, le Directeur Général de la Sûreté Nationale, est un membre du Comité Stratégique de la cybersécurité, dont la mission est de d'élaborer les orientations stratégiques du Maroc dans le domaine de la cybersécurité .

La DGSN est également représentée au sein du Comité de gestion des crises et événements cyber-

nétiques majeurs, instituée auprès du Comité stratégique de la cybersécurité.

POLICE

Qu'en est-il de la promotion de la culture de la SSI au sein de la DGSN?

Le facteur humain est la clé dans toute stratégie de cybersécurité et peut être source de vulnérabilité pouvant impacter la sécurité des systèmes d'information. C'est pour cela que la DGSN a fait de la sensibilisation de son personnel, l'un des axes stratégiques de sa politique de sécurité de l'information, afin de promouvoir et consolider la culture de sécurité des SI.

C'est ainsi qu'une charte de la sécurité de l'Information a été établie et remise à l'ensemble du personnel, notamment aux nouvelles recrues. Aussi, la SSI fait partie intégrante de la formation de base, pour bien imprégner les nouvelles recrues des principes de sécurité de l'information, des risques et des conséquences, ainsi que les bonnes pratiques en la matière.

> *La DGSN a fait de la sensibilisation de son personnel, l'un des axes stratégiques de sa politique de sécurité, afin de promouvoir et consolider la culture de sécurité des SI.*

Dans le même esprit, la DSSI établit un plan annuel de sensibilisation, aussi bien au niveau central que déconcentré, et organise des séminaires à l'Institut Royal de Police, au profit des responsables et des fonctionnaires de police tous grades confondus. Les thématiques abordées sont diverses et portent sur les normes et les directives en relation avec la SSI, les règles de bonne hygiène informatique, les risques, etc. L'objectif étant de renforcer les connaissances du personnel, de rappeler les bonnes mesures, et d'ancrer in fine, la culture de sécurité de l'information dans le quotidien de ces fonctionnaires.

Depuis, l'instauration de ce plan de sensibilisation en 2015, le nombre de fonctionnaires de police ayant bénéficié de ces sessions va crescendo, bien qu'il ait été impacté par la COVID-19. On est passé de 334 fonctionnaires en 2005 à 4.140 en 2021 ■

DOSSIER

© 2021 DGSN

La lutte contre la cybercriminalité..

composante essentielle de la stratégie de cybersécurité pour un cyberespace plus sûr

La révolution numérique et l'essor fulgurant des nouvelles technologies, telles que la robotique, les objets connectés, l'intelligence artificielle ou autres, ont transformé radicalement la société dans sa globalité. Si ces technologies sont fort utiles dans divers secteurs d'activités, elles génèrent néanmoins des risques, constituant des « opportunités » pour les cybercriminels, qui se sont appropriés ces technologies, pour perpétrer leurs méfaits et générer des bénéfices, tout en gardant leur anonymat.

Des milliers de personnes sont quotidiennement connectées via les ordinateurs, tablettes et smartphones, pour diverses raisons, publient du contenu et des données personnelles sur les réseaux sociaux. Des institutions publiques et des entreprises se sont, elles aussi, ouvertes sur le cyberespace, un territoire où pullulent des virus informatiques et des dangers de tous genres et dans lequel des prédateurs, des cybercriminels et des pirates, sont à l'affût de toute proie vulnérable. En janvier 2021, ils étaient 27 millions Marocains à utiliser Internet et 22 millions sur les réseaux sociaux (d'après l'Agence Nationale de Réglementation des Télécommunications). L'envoi d'un e-mail d'hameçonnage, imitations «presque» parfaites de sites Web, vols de données personnelles pour demander des rançons, utilisation de votre machine à votre insu pour générer de la cryptomonnaie, utilisation de noms de domaines déguisés, etc., les modes opératoires sont divers et variés. Le crime a pris une autre dimension, celle du virtuel, où les frontières sont abolies. Le cyberespace est devenu alors le théâtre de la commission croissante d'infractions de toutes natures, qui deviennent de plus en plus sophistiquées. Des cybercriminels à l'affût d'une cible vulnérable ou de systèmes d'information défaillants, aux fins d'extorsion, de chantage, de vengeance, d'idéologie et d'endoctrinement, etc. Car si le territoire a bien changé, les motivations, elles, sont restées inchangées, mais sont devenues encore plus graves. En effet, l'impact est d'autant plus conséquent quand il s'agit de données stratégiques ou sensibles, risquant de mettre en péril ou de tétaniser complétement le fonctionnement d'infrastructures vitales au sein même d'un Etat.

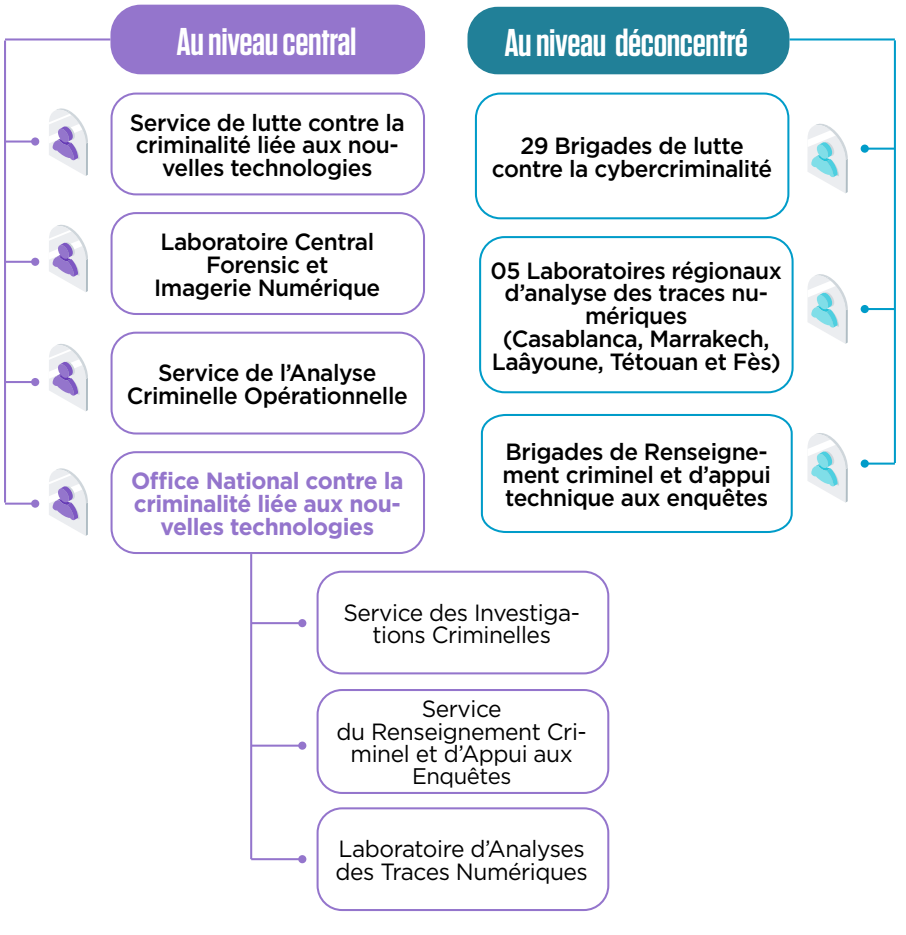
Pour protéger le cyberespace de ces personnes malveillantes, les services de police se sont vus dans l'obligation de s'adapter et d'adapter leurs méthodes de travail et de s'approprier eux aussi, les nouvelles technologies, pour détecter ces crimes, identifier les auteurs et les présenter à la justice, afin de réduire ainsi les surfaces d'attaques.

La lutte contre la cybercriminalité est devenue alors, une composante fondamentale de toute stratégie de cybersécurité, pour traquer les cyberdélinquants et cybercriminels, et les mettre hors d'état de nuire, pour un cyberespace plus sûr et sécurisé.

Des structures dédiées à la lutte contre la cybercriminalité

Bien consciente de l'ampleur que prend le fléau de la cybercriminalité et soucieuse d'assurer la protection de la population contre cette forme criminalité qui a investi le cyberespace, la DGSN s'est adaptée et s'est organisée, il y a bien quelques années déjà, pour la prévention et la lutte contre la cybercriminalité, par la mise en place de structures centrales et déconcentrées de lutte contre la cybercriminalité, de laboratoires d'analyses des traces numériques et d'unités de renseignement criminel. Cette structuration a été accompagnée par le recrutement de profils adaptés, l'acquisition de moyens technologiques et la mise en place de procédures standardisées. Et parce que la cybercriminalité n'a pas de frontières, la DGSN a développé et fructifié les partenariats et la coopération tant à l'échelon national qu'international, afin d'appréhender et d'identifier les cybercriminels pour les traduire en justice. La DGSN, institution qui ne cesse d'innover, a développé les campagnes de sensibilisation en milieu scolaire, pour prémunir la jeune population des dangers pouvant les guetter, dont les dangers d'Internet. Cette sensibilisation est assurée également à l'occasion des journées portes ouvertes de la Sûreté Nationale, où des policiers spécialistes viennent expliquer aux jeunes, les dangers d'Internet et leur donner des conseils, afin d'éviter d'être une victime dans le cyberespace.

Réseau de la DGSN de lutte contre la cybercriminalité



Pour mettre la lumière sur la composante de lutte contre la cybercriminalité de la DGSN, la Revue de Police s'est entretenue avec des cadres de l'Office National contre la Criminalité liée aux Nouvelles Technologies «**ONCLNT**», relevant de la Brigade Nationale de la Police Judiciaire «BNPJ», une entité d'élite, chargée de la lutte contre la criminalité transnationale sous toutes ses formes et manifestations et traitant les grandes affaires à ramifications nationales et internationales.

L'Office National contre la Criminalité Liée aux Nouvelles Technologies est l'un des quatre offices constituant la Brigade Nationale de la Police Judiciaire, qui vient d'emménager en 2021, dans un bâtiment flambant neuf à Casablanca, répondant aux normes de construction et de sécurité, les plus actuelles régissant les bâtisses du genre.

Cet Office revêt une spécificité toute particulière, dans la mesure où il s'agit d'une structure intégrée rassemblant les composantes clés et complémentaires impliquées dans la gestion des affaires dans lesquelles la technologie est un outil ou un vecteur de commission des infractions, apportant ainsi, son appui à l'ensemble des Offices de la BNPJ. Il s'agit en l'occurrence de l'aspect investigations, de l'analyse forensique et enfin, de l'analyse du renseignement criminel.

Une organisation intelligente, permettant de gagner en rapidité et en efficacité opérationnelle. Une entité dont l'action est transversale, impliquée dans quasi toutes les affaires confiées à la BNPJ, puisque la composante technologie est prégnante.

Mohamed SASSI

Commissaire Divisionnaire et Chef de l'Office national contre la criminalité liée aux nouvelles technologies à la Brigade Nationale de la Police Judiciaire, depuis 2018, date de sa création.

Il a rejoint les rangs de la Sûreté Nationale en 1995 en tant qu'Officier de Police et a directement été affecté à la BNPJ, après sa sortie de l'Institut Royal de Police à Kénitra. Au sein de la BNPJ, unité d'élite en matière d'investigations judiciaires, ce jeune policier a affiné et a développé ses compétences en tant qu'enquêteur dans diverses affaires ayant trait à la criminalité financière, au trafic de drogues, à la migration irrégulière, etc., puisqu'il a exercé dans l'ensemble des Offices de la BNPJ. Après une formation pointue sur l'analyse criminelle opérationnelle, dans le cadre de la coopération avec la police fédérale Belge, il fut nommé en 2014, chef du Service collecte et analyse de l'information, toujours à la BNPJ. Le sérieux de ce gradé et son engagement indéfectible, conjugués à l'expertise développée au fil des années dans le domaine technique et cybernétique, lui ont valu sa nomination en 2018, en tant que Chef de l'Office national contre la criminalité liée aux nouvelles technologies «ONCLNT».

Quel rôle occupe l'Office dans la lutte contre la criminalité liée aux nouvelles technologies ?

Permettez-moi tout d'abord de dresser un bref aperçu de l'Office que j'ai l'honneur et le plaisir de diriger. L'Office national contre la criminalité liée aux nouvelles technologies «ONCLNT», est le plus *jeune* des Offices de la BNPJ, qui a vu le jour en 2018. Auparavant, la lutte contre la cybercriminalité à la BNPJ, était l'apanage d'une cellule, qui a évolué par la suite en service. Il était, alors naturel qu'avec la montée fulgurante des affaires de cybercriminalité, de revoir la structure organisationnelle, afin d'être en mesure d'appréhender ce fléau avec l'efficacité et la rapidité requises. En fait, l'Office fait partie du dispositif intégré de la DGSN, dans le domaine de la lutte contre la criminalité liée aux nouvelles technologies. Notre action porte sur les grandes affaires à portée nationale et internationale ou qui revêtent une certaine complexité. Cela étant, nous travaillons bien entendu dans une synergie et une totale complémentarité.

L'Office est constitué de trois services, le service des investigations criminelles, le laboratoire d'analyse des traces numériques et le service du renseignement criminel et d'appui aux enquêtes. Cette structure intégrée et cohérente, nous permet de mettre ensemble toutes les données et informations, tant opérationnelles que techniques, dont nous disposons, au service du directeur d'enquête en charge de l'affaire. Car, il faut le préciser, dans ce domaine, ces trois composantes se complètent les unes les autres pour donner du sens aux différentes données, celles issues du terrain, celles issues des investigations sur Internet ou des supports numériques, avec celles issues d'autres sources, telles que les opérateurs de téléphonie, les fournisseurs d'accès à Internet ou autres. Il faut préciser que notre action et notre démarche se font toujours sous la supervision du Parquet compétent et toutes nos réquisitions judiciaires sont visées par le Ministère Public.

Quel est l'ampleur de la criminalité liée aux nouvelles technologies au Maroc ?

La numérisation de notre quotidien et la démocratisation d'Internet ont ouvert la voie à une nouvelle forme de criminalité qui est facilitée par ces technologies ou qui l'utilise carrément. Cette forme de criminalité qui, d'ailleurs, ne cesse de se sophistiquer avec de nouveaux modes opératoires qui font usage des dernières technologies sur le marché. Des logiciels malveillants, aux Botnets, en passant par les Rançongiciels, le Cryptojacking et bien d'autres, les modes opératoires sont nombreux et les cybercriminels ne cessent d'innover pour perpétrer leurs méfaits dans un anonymat total.

Bilan global de lutte contre la cybercriminalité en 2021

Nombre d'affaires traitées par les diverses entités de la DGSN

5.275

Contenus illicites

3.533 publications

Affaires de sextorsion

498 affaires

270 maîtres-chanteurs arrêtés
508 victimes identifiées, dont
95 de nationalités étrangères

tales, causant des préjudices colossaux, financiers, de réputation, psychologiques, etc. Le cyberespace est devenu alors le théâtre de prédilection de ces cybercriminels, qui y ont transposé leurs activités illégales de tous genres, faisant fi des frontières, et prospérant dans le Web invisible avec l'utilisation des cryptomonnaies, afin de rendre la traçabilité de leurs mouvements financiers difficile voire impossible. Aujourd'hui, avec 4,66 milliards d'utilisateurs d'Internet dans le monde (Source : We are social et Hootsuite), l'augmentation du nombre de transactions en ligne, le développement des objets connectés, etc., la cybercriminalité ira sans aucun doute en exponentielle, constituant ainsi un réel défi pour les services de sécurité du monde entier, qui doivent adapter la réponse et renforcer la coopération opérationnelle internationale, pour faire face à ce fléau. Et le Maroc ne fait pas exception.

Pour vous donner une idée, étant précisé qu'il s'agit uniquement de la partie visible de cette forme de criminalité, le nombre réel d'affaires dépasserait certainement ces chiffres enregistrés. Au cours de l'année 2021, les services de la Sûreté Nationale ont traité 5.275 affaires et ont pu détecter sur la base d'un travail anticipatif de veille, 3.533 publications de contenus illicites. En relation avec la sextorsion, 498 affaires ont été traitées, ayant mené à l'arrestation de 270 maîtres-chanteurs et à l'identification de 508 victimes, dont 95 de nationalités étrangères. Concernant les affaires de sextorsion en général, ainsi que la publication de vidéos et de photos à caractère pédopornographiques, nous avons travaillé sur plusieurs affaires signalées par les autorités judiciaires ou policières

étrangères relevant de pays disposant de dispositifs très développés dans la détection de ces publications, telles que les Etats-Unis, l'Allemagne, la France, l'Espagne, les Pays-Bas, la Suisse, etc.

Un autre point qu'il me paraît important de souligner, concerne la COVID-19 qui a eu aussi un impact sur le nombre d'affaires de cybercriminalité enregistrées, surtout lors de la période de confinement où les téléphones mobiles et Internet étaient les seuls liens avec le monde extérieur.

POLICE

Pouvez-vous nous en dire plus par rapport à l'impact de la crise pandémique sur les affaires de cybercriminalité ?

Durant la période de confinement, nous avons constaté une hausse exponentielle des affaires de cybercriminalité, qui a constitué une «opportunité» en or pour les cybermalfaiteurs. Ces criminels ont, en effet, tiré profit de cette situation et ont multiplié les escroqueries et les arnaques dans le cyberespace, notamment l'hameçonnage, le vol de données personnelles, le chantage et l'extorsion, la sextorsion, la publication de vidéos à caractère pédopornographique, ainsi que la commercialisation de produits nocifs à la santé et la publication de fake news au sujet de la pandémie.

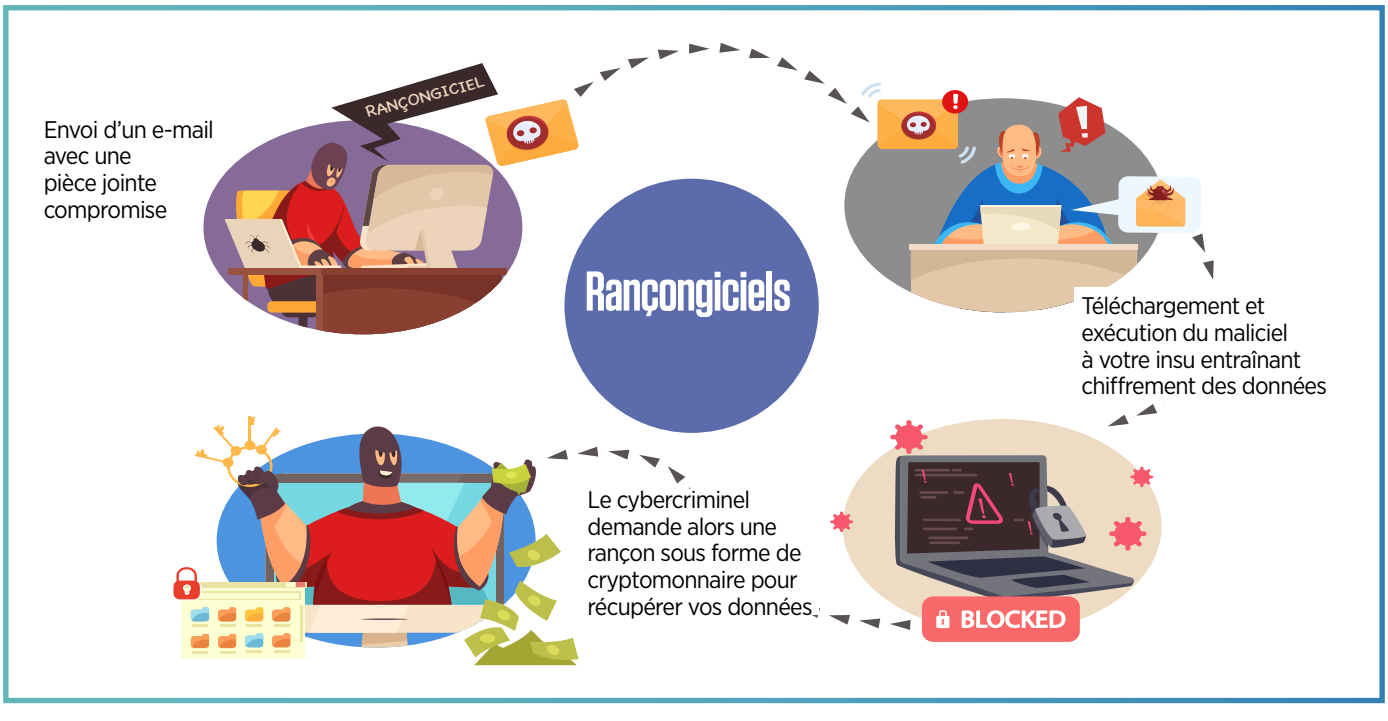
Durant la crise pandémique, les cybercriminels ont fait usage de la panique et de la peur de la population face à cette crise, par l'utilisation du terme « coronavirus» ou « covid-19 » pour créer de nouveaux noms de domaines, pour diffuser des logiciels malveillants ou pour mener des campagnes de spam et de phishing.

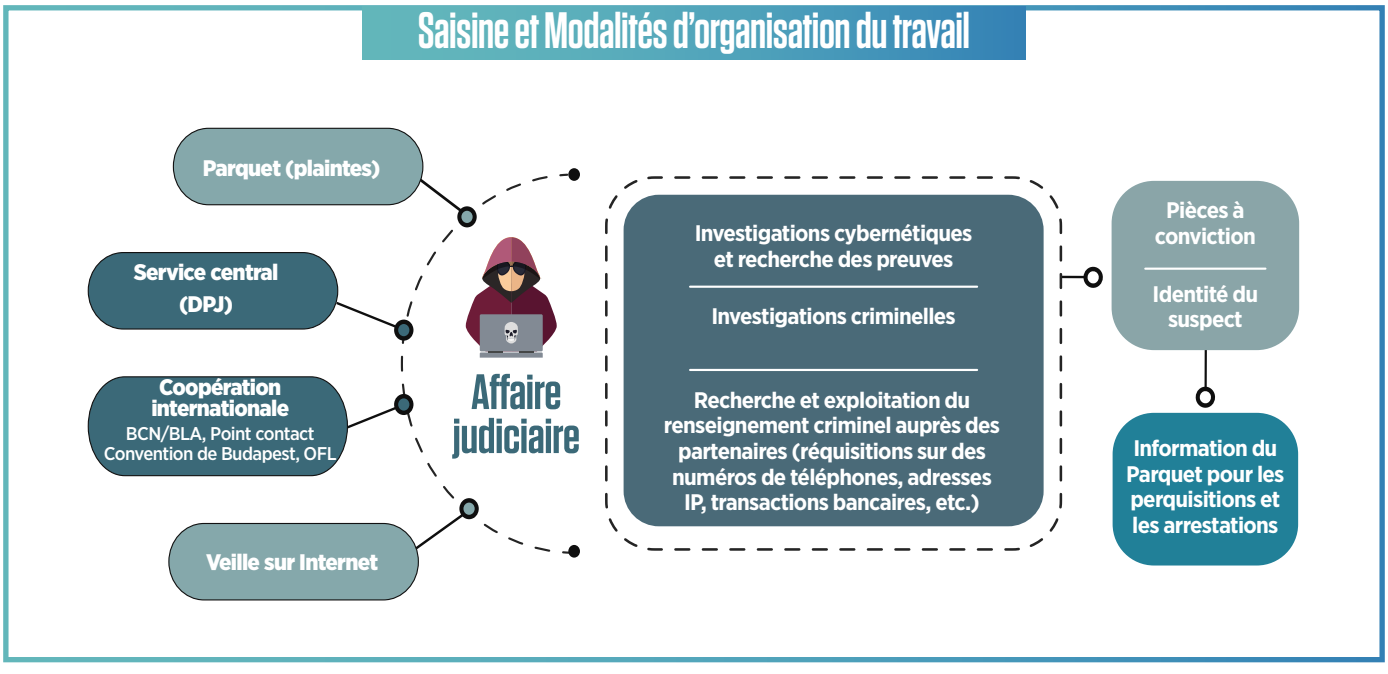
Les victimes ciblées recevaient des courriels les incitant à cliquer sur des liens, et téléchargeaient alors à leur insu des maliciels, conçus pour infiltrer les ordinateurs et appareils mobiles, et y effectuer des activités non autorisées, tels que le vol de données personnelles ou leur chiffrement, en vue de demander par la suite une rançon. Imaginez si ces attaques ciblaient des établissements hospitaliers et d'autres institutions stratégiques, ce qui va les rendre inopérables et créer ainsi de grands dégâts. L'application CovidLock, en est l'exemple parfait.

CovidLock..
Une application «déguisée» en rançongiciel

Nous avons été saisis par la DGSSI, d'une affaire de rançongiciel, relative à une application développée par un ingénieur informaticien marocain, baptisée **CovidLock,** téléchargeable sur les systèmes d'exploitation iOs et Android.

Cette application, paraissait à première vue anodine pour tout le monde, et donnait une vue globale sur l'état de la pandémie dans le monde et proposait même des conseils sur la conduite à tenir face à la COVID- 19. Mais, en réalité, il s'agissait d'un malware, qui une fois téléchargé, bloque l'accès à l'appareil via un mot de passe généré automatiquement pour mettre la main sur le contenu de l'appareil. Pour le débloquer, les victimes devaient payer une rançon en cryptomonnaie. Grâce aux investigations minutieuses que nous avions menées, nous avons pu identifier l'auteur et l'interpeller.





La lutte contre la cybercriminalité nécessite des profils techniques de pointe, comment se fait le développement de ces compétences et qu'en est-il de leur formation ?

Tout à fait, et la DGSN dans sa stratégie « RH », procède chaque année, au recrutement de profils techniques divers, des docteurs, des ingénieurs et des techniciens dans les diverses spécialités scientifiques, informatique, réseaux, sécurité, etc., dont les compétences ne cessent d'être perfectionnées et aiguisées par la formation continue et la spécialisation, aussi bien au Maroc qu'à l'étranger. Dans ce domaine qui connaît une évolution fulgurante, le perfectionnement de nos cadres est essentiel pour être au parfum de l'état de l'art en matière de technologies, de menaces, de nouveaux modes opératoires, et aussi de nouvelles techniques d'enquêtes.

Au niveau de l'Office, nous avons un « cocktail » de spécialités, des juristes, des ingénieurs, des techniciens spécialisés et des data analystes, qui travaillent tous ensemble dans une affaire. Les formations sont très diversifiées et portent sur les techniques d'investigation sur Internet, la gestion de la scène de crime numérique et de la preuve électronique, la veille et la détection des infractions cybernétiques, l'analyse criminelle opérationnelle, les techniques d'exploitation des données, la cryptomonnaie, la protection des enfants contre les actes d'abus et d'exploitation sexuels en ligne, la cybersécurité, les nouvelles menaces dans le cyberespace et les nouveaux modes opératoires, etc. Nous assurons également, dans le cadre de la coopération Sud-Sud, des formations au bénéfice de policiers relevant de pays amis.

Cela étant, en plus du renforcement des compétences, la DGSN a investi dans les outils d'analyse et d'investigations. Aujourd'hui, nous disposons d'équipements et d'outils modernes et reconnus à l'échelon internationale, en matière de veille, d'analyse et d'exploitation forensiques. Nous travaillons également avec des procédures bien établies et standardisées, dans le respect du cadre légal de traitement de la preuve, de son intégrité et de sa traçabilité.

Dans la pratique, comment est organisé le travail au sein de l'Office ?

Au sein de l'Office, nous avons la chance d'avoir les composantes clés réunies, l'enquêteur, le data analyste et le spécialiste en digital forensic. Ça nous permet de gagner en efficacité opérationnelle. Car une enquête en cybercriminalité évolue en chaîne et implique des données d'ordre juridique et procédural, mais également technique. En matière d'enquête des affaires de cybercriminalité, c'est la conjugaison de la mise en œuvre de divers outils et méthodes qui permet de solutionner l'affaire, d'identifier le ou les auteurs et de matérialiser les preuves tangibles et scientifiques de la commission de l'infraction. C'est pour cela que l'apport du laboratoire d'analyse des traces numériques et le service du renseignement criminel et d'appui aux enquêtes, revêtent une importance vitale et durant toutes les étapes de l'investigation. Les résultats du flux important de données issues des investigations en ligne ou sur des supports numériques, sont conjugués avec les données techniques issues des réquisitions judiciaires avec les partenaires concernés, notamment les opérateurs de téléphonie et les fournisseurs d'accès à Internet, ainsi que les données

opérationnelles issues du terrain, nous permettent de dégager des liens intéressants entre cette grande masse de données, de déceler des tendances et d'échafauder des hypothèses, à même d'orienter les enquêteurs.

Nous pouvons être saisis d'une affaire par les autorités judiciaires, par la Direction de la Police Judiciaire ou par des partenaires étrangers avec lesquels nous entretenons des relations de coopération, en l'occurrence le Bureau Central National Interpol-Rabat, le Bureau de Liaison Arabe, les Officiers de Liaison accrédités au Maroc ou le point de contact I-24/7 de la Convention de Budapest sur la cybercriminalité. Comme nous pouvons déclencher les investigations d'initiative, sur la base du travail de veille que nous menons quotidiennement, pour détecter toutes sortes d'activités ou de contenus illicites. Il faut préciser une chose très importante, chaque étape de notre travail se fait sous la supervision et l'aval du Parquet compétent.

Extrait du rapport d'Interpol sur les cybermenaces en Afrique en 2021, qui met en valeur l'apport des services de la DGSN, ayant mené à l'arrestation d'un cybermalfaiteur connu sous le pseudonyme de Dr. HEX

ÉVALUATION 2021 DES CYBERMENACES EN AFRIQUE

3.2 Opération Lyrebird

INTERPOL | GROUP-IB

En 2021, un présumé cybermalfaiteur très actif a été appréhendé au Maroc à la suite d'une enquête de deux ans menée conjointement par INTERPOL, la police marocaine et Group-IB. Agissant sous le pseudonyme de « Dr Hex », le suspect aurait, des années durant, ciblé des milliers de victimes sans méfiance en se livrant à l'hameçonnage, à la fraude et au piratage de cartes bancaires à l'échelle mondiale.

Il est aussi accusé de s'être livré au « défacement » de nombreux sites Web en en modifiant la présentation et le contenu, et d'avoir ciblé des entreprises de télécommunications francophones, plusieurs banques et des multinationales en utilisant des logiciels malveillants. Par ailleurs, le suspect aurait contribué à développer des kits de piratage de cartes bancaires et d'hameçonnage, qui étaient ensuite vendus à d'autres individus via des forums en ligne, afin de leur permettre de mener des campagnes similaires de maliciels.

Les logiciels malveillants étaient ensuite utilisés pour usurper l'identité de banques en ligne, ce qui a permis au suspect et à d'autres de voler des informations sensibles et d'escroquer des personnes sans méfiance à des fins de profit. Le préjudice causé aux particuliers et aux entreprises était ensuite publié sur Internet, afin de faire la publicité de ces services malfaisants.

Dans le cadre de l'opération Lyrebird, la Direction de la Cybercriminalité d'INTERPOL a travaillé en étroite coopération avec Group-IB et la police marocaine par l'intermédiaire du Bureau central national du Maroc à Rabat, pour enfin localiser et appréhender l'individu, qui fait toujours l'objet d'une enquête.

Réseau 24/7 de la Convention de Budapest..

Le réseau des points de contact 24/7, est un mécanisme établi en vertu de l'article 35 de la Convention de Budapest sur la cybercriminalité.

La Convention sur la cybercriminalité, communément dite de Budapest, a été signée en 2001 à Budapest en Hongrie et est entrée en vigueur en 2003. Il s'agit d'un traité international, dont l'objectif est d'assurer la protection des usagers du cyberespace contre la cybercriminalité, notamment par l'adoption d'une législation appropriée, le renforcement des cybercapacités et l'amélioration de la coopération internationale. 67 pays ont ratifié cette Convention, dont le Maroc, qui a déposé les instruments d'adhésion à la Convention et son Protocole additionnel en 2018. La Convention de Budapest a été publiée dans le Bulletin Officiel, par le Dahir n° 1-14-109 du 21 rejeb 1441 (16 mars 2020).

En vertu de l'article 35 de cette Convention, chaque Partie désigne un point de contact joignable 24h/24 et 7j/7, afin d'assurer une assistance immédiate et accélérée des procédures d'investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique. Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée.

Le Maroc a désigné le Service de Lutte contre la Criminalité liée aux Nouvelles Technologies (SLCNT) relevant de la Direction de la Police Judiciaire à la DGSN, et le Pôle de suivi des affaires pénales et la protection des catégories spéciales relevant de la présidence du ministère public.

Vous avez parlé de mécanismes de coopération internationale, pouvez-vous nous en dire plus et qu'en est-il des partenariats ?

La coopération internationale est essentielle pour essayer d'endiguer le phénomène de la cybercriminalité. En effet, dans le cyberespace, les cybercriminels peuvent vivre dans un pays et commettre leurs méfaits dans un autre, en laissant les preuves dans un autre pays. D'où la nécessité d'une coopération policière internationale avec les pays partenaires et aussi le secteur privé. La coopération internationale se matérialise par une multitude de mécanismes nous permettant de recueillir des informations dans le cadre de l'entraide internationale, dont les plus importants sont: le Bureau Central National Interpol-Rabat, le Bureau de Liaison Arabe et le point de contact 24/7 de la Convention de Budapest sur la cybercriminalité.

Nous avons également tissé des partenariats avec plusieurs établissements au niveau national, dont notamment les banques, les assurances, les agences de transfert de fonds, le cadastre, les fournisseurs d'accès à Internet, les opérateurs de téléphonie, etc. Le succès d'une enquête en cybercriminalité est conditionné souvent par des informations détenues par ces agences que j'ai citées.

Afin d'illustrer l'importance de cette coopération, nous avons pu identifier et arrêter un hacker marocain recherché par Interpol, portant comme pseudonyme «DR HEX », qui s'adonnait au piratage de comptes bancaires et d'informations à caractère personnel, pour s'offrir divers services, en utilisant ces cartes bancaires, et ce, depuis plusieurs années. Ce cybermalfaiteur avait pris pour cibles, des milliers de victimes, ainsi que des institutions étrangères pendant une dizaine d'années en adoptant la technique d'hameçonnage. Nous avons travaillé en étroite collaboration avec Interpol et une entreprise spécialisée en cybersécurité, et cet échange a permis de mettre fin aux activités illégales de ce cybercriminel.

Quels conseils donneriez-vous à nos lecteurs, pour éviter qu'ils ne soient victimes de ces cybercriminels ?

Le cyberespace est un territoire à part entière, où les cybercriminels traquent les vulnérabilités pour piéger leurs victimes. Aujourd'hui, nous fournissons beaucoup d'informations sur nos vies, nos activités, nos familles, nous effectuons des achats en ligne, nous échangeons en ligne et souvent avec des personnes qui prétendent être celles qui ne le sont pas réellement. La prudence est de mise, car si la population est sensibilisée sur les risques, le nombre d'affaires de cybercriminalité ira certainement en diminuant. C'est pour cela que la sensibilisation est très importante. La DGSN, institution citoyenne, s'est inscrite dans cette perspective, il y a quelques années déjà, en organisant chaque année des campagnes de sensibilisation dans les établissements scolaires sur les dangers d'Internet, qui ont atteint pour l'année scolaire 2020-2021, plus de 6.000 établissements au bénéfice de 240.000 élèves.

Il faudrait adopter par tout un chacun des normes d'une cyberhygiène, qu'on pourrait facilement mettre en œuvre, afin qu'on puisse mener nos activités dans le cyberespace de manière plus sûre et sécurisée. Ces mesures concernent la protection de nos comptes e-mails et sur les réseaux sociaux, nos ordinateurs et nos smartphones et aussi notre réseau WIFI. Pour ce faire, nous devons veiller à l'installation d'anti-virus et à les mettre à jour, à choisir des mots de passe complexes et différents pour chaque application, à ne pas cliquer sur des liens suspects, à ne pas partager son WIFI avec des personnes inconnues, etc ■

Quelques cyberconseils

DOSSIER

L'analyse des traces numériques...

une composante «experte» qui fait parler la cyberpreuve

© 2021 DGSN

Les investigations en matière de cybercriminalité associent les fondamentaux de la procédure judiciaire à des composantes techniques. L'objectif est d'identifier et d'interpeller les cybercriminels qui utilisent le numérique et le cyberespace pour commettre leurs infractions et de matérialiser la preuve qui les incrimine.

L'enjeu majeur face à l'évolution grandissante des technologies et la sophistication des modes opératoires des cybercriminels, est de pouvoir matérialiser la preuve, qui va les incriminer. Une preuve volatile, pouvant être modifiée ou effacée à distance. C'est le travail des experts du Laboratoire d'Analyse des Traces Numériques. Des experts qui mettent à jour leurs compétences et assurent une veille technologique permanente pour être au parfum des nouveautés. Des experts qui bénéficient de manière soutenue de sessions de formation continue et de spécialisation au niveau national et international pour maintenir un haut niveau d'expertise et d'être à la hauteur des enjeux et défis posés par cette nouvelle forme de criminalité.

Marouane HEJJOUJI

Il est Commissaire Divisionnaire et Ingénieur en Informatique, Chef du Laboratoire d'Analyse des Traces Numériques à l'Office National contre la Criminalité liée aux Nouvelles Technologies à la BNPJ. Lauréat de l'Université AL AKHAWAYNE, il est titulaire d'un diplôme d'Ingénieur en Informatique. Il a intégré la DGSN en 2007 et a été affecté à la Brigade Nationale de la Police Judiciaire, en tant que Chef de la Cellule de Lutte contre la Cybercriminalité. Cellule qui été élevée au rang d'un Service en 2013 et dont il a été le Chef. En 2018, avec la création de l'Office National contre la Criminalité liée aux Nouvelles Technologies, il fut nommé chef du Laboratoire d'Analyse des Traces Numériques. Ce jeune gradé de police a pu au fil des années acquérir une grande expertise dans le domaine du digital forensique et maîtriser les techniques les plus fines, même dans des affaires revêtant une certaine complexité, pour traquer les cybercriminels dans le cyberespace. Aucune investigation n'est impossible, elle constitue toujours un challenge qui est toujours excellemment relevé par cette équipe de cyberexperts.

POLICE

En quoi consiste le travail du laboratoire d'analyse des traces numériques ?

Permettez-moi tout d'abord d'apporter une précision par rapport aux infractions cybernétiques. On distingue deux catégories. Il y a celles qui sont directement liées à la technologie, plus explicitement celles où la technologie est la cible, telles que le déni de service, l'effacement d'un site web, etc. Et les autres qui sont facilitées par les technologies, c'est-à-dire que la technologie constitue un vecteur pour commettre les infractions, comme par exemple les escroqueries en ligne, la fraude au président, les atteintes aux systèmes de traitement automatisé de données, les vols de données par ingénierie sociale, les rançongiciels, etc. Cette dernière forme est la plus fréquente.

Dans les deux cas de figure, les infractions sont commises à distance et de façon anonyme. Les motivations peuvent être diverses, politiques, notoriété et image, financières, etc., mais les la cupidité demeure la motivation la plus prégnante, qui anime ces cybercriminels. En outre et pour garder l'anonymat et éviter la traçabilité des mouvements financiers, les cybercriminels mènent leurs méfaits au niveau des réseaux fermés (Dark web) et sollicitent leurs rétributions en monnaie virtuelle, la cryptomonnaie.

Au niveau du laboratoire, nous effectuons un travail d'initiative, en sillonnant Internet pour détecter tout signal lié à une

activité illégale ou des contenus illicites, nous procédons à la recherche et à l'extraction de la preuve numérique incriminant les faits et nous en informons les Officiers de Police Judiciaire, pour entamer la procédure, après accord du Parquet compétent. Nous travaillons également sur les supports numériques physiques, ordinateurs, DVR, CD, terminaux mobiles, supports amovibles, smartphones, etc., saisis à l'occasion des perquisitions judiciaires ou sur les scènes de crime, afin d'en extraire les données et rechercher les éléments de preuves en relation avec l'affaire.

Dans les deux cas, nous intervenons en appui technique aux enquêtes, pour apporter la preuve matérielle scientifique nécessaire à la manifestation de la vérité, consolidant ainsi, le droit constitutionnel à un procès équitable.

Pour mener à bien notre mission, nous avons l'immense chance d'avoir emménagé dans des locaux flambants neufs où nous disposons de plateaux d'investigations forensique numérique dotés de matériels de dernière génération et les plus utilisés dans les sciences légales au niveau international.

POLICE

Comment vous opérez dans la pratique ?

Notre principale action est de mener des investigations cybernétiques et de procéder à l'analyse des traces numériques, sur des affaires ayant une ampleur nationale ou internationale, dont nous sommes saisis, soit par l'autorité judiciaire, les services de la DGSN ou via la coopération internationale. Nous recherchons et collectons les preuves de la commission des infractions et nous coordonnons notre action avec l'Officier de Police Judiciaire, qui n'est en fait que le directeur de l'enquête.

Notre champ de compétence est national et nous prenons en charge les affaires ayant plusieurs ramifications. La lutte contre la cybercriminalité est un travail d'équipe, via un échange continu avec l'enquêteur et le service du renseignement criminel. Et la conjugaison de ce triptyque, nous permet de comprendre et d'établir les faits, faire des rapprochements et orienter l'enquêteur sur la bonne piste à suivre. On gagne alors en efficacité opérationnelle.

L'équipe du Laboratoire est composée d'ingénieurs et de techniciens spécialisés, triés sur le volet et bénéficiant de formations pointues en matière de veille sur Internet, de nouvelles menaces «cyber», ainsi que le traitement et l'analyse de la preuve numérique. Nous travaillons également avec des procédures standardisées reconnues à l'échelon international. Toutes les preuves sont recueillies selon les normes de préservation de leur intégrité et traçabilité, en utilisant des conditionnements spécifiques à chaque type de preuve.

S'il s'agit par exemple d'un GSM, on le transportera dans une cage de Faraday, afin de l'isoler et d'éviter ainsi tout risque de modification de son contenu, etc. Nous réalisons également une copie intégrale bit à bit des supports numériques, objets des expertises, avec des logiciels forensiques dédiés, en plus d'un blocage en écriture. Nous réalisons nos expertises sur la copie, afin de rechercher d'éventuelles preuves, tout en veillant à garder le matériel initial intact, gage de traçabilité et d'intégrité. C'est très important.

Nous disposons également de capacités d'expertise et d'outils performants, qui nous permettent d'expertiser des supports chiffrés, cassés ou dont le contenu a été supprimé. C'est notre plus-value en tant qu'experts.

Quand il s'agit de pièces à conviction sur Internet, nous réalisons des captures d'écran et nous établissons un procès-verbal de constatation, en précisant la date, l'URL, etc. Concernant les vidéos ou les messages audio, nous les transcrivons dans leur intégralité dans le procès-verbal technique qui sera joint à la procédure. Un travail très minutieux.

- ***Déni de service :*** Envoi massif de requêtes à un site internet, provoquant ainsi, sa saturation et son indisponibilité.
- ***Défacement :*** Modifications non sollicitées d'un site Internet.
- ***Rançongiciel*** : Chiffrement de données sur ordinateurs, tablettes ou smartphones et demande d'une rançon pour les déchiffrer.
- ***Minage :*** Détournement de la puissance de calcul des ordinateurs pour générer de la cryptomonnaie.
- ***Fraude au président :*** L'escroc se fait passer pour le président d'une société, et exige d'un employé le versement rapide et confidentiel d'une somme d'argent de la société, sur un compte basé à l'étranger.

Investigations et traitement de la cyberpreuve

L'intégrité et la traçabilité de la cyberpreuve.. **principes qui guident nos actions**

Dans la pratique, le matériel informatique saisi, après le prélèvement selon une procédure établie, passe d'abord dans la salle de préservation des pièces à conviction, dont nous disposons à la BNPJ, avant de commencer l'expertise proprement dite. C'est un nouveau mécanisme mis en place au sein de l'ensemble des commandements du Royaume, pour assurer l'intégrité et la traçabilité des preuves. C'est primordial dans le cadre de la consolidation du droit constitutionnel à un procès équitable. Son principe est que toutes les preuves collectées par les techniciens de scènes de crime, soient acheminées tout d'abord à la salle de préservation des pièces à conviction, une sorte de grand coffre-fort, sécurisé avec une porte blindée et des caméras de surveillance, ainsi qu'une chambre froide, dédiées à la réception et le stockage de tous les types de preuves. Le chargé de cette salle, est tenu de vérifier leur conditionnement et leur intégrité, et les entreposer selon leurs natures dans l'endroit approprié. Elles sont ensuite prises en charge par le service qui va effectuer l'expertise, qui est tenu par la suite de les restituer à la salle de préservation après la fin de l'expertise. Cette procédure traduit le volonté ferme de la DGSN de mettre tous les garde-fous possibles pour assurer l'intégrité de la preuve, qui va servir à incriminer ou innocenter un individu.

Le travail effectué est sanctionné par la rédaction d'un rapport d'expertise détaillé qui sera joint aux actes de procédure réalisés par l'OPJ.

POLICE

Quel a été le bilan du laboratoire d'analyses des traces numériques de la BNPJ ?

Nous faisons partie du réseau de la DGSN de lutte contre la cybercriminalité, qui a pu traiter au titre de l'année 2021, 5.275 affaires. Au niveau de la BNPJ, nous avons pu traiter 111 grandes affaires de criminalité liée aux nouvelles technologies, dont 47 liées aux menaces sur Internet et 22 affaires relatives à la cyberpédophilie.

© 2021 DGSN

Je tiens à préciser par rapport au volet de la protection des enfants sur Internet, auquel la DGSN accorde une attention toute particulière, que nous avons des unités dédiées, disposant d'outils et d'équipements sophistiqués qui ne travaillent que sur ce volet et qui assurent la veille pour détecter tout signal révélateur de cette activité en ligne, telle que par exemple le partage de fichiers à caractère pédopornographique. En ce sens, nous avons traité une affaire, en étroite collaboration avec le FBI, relative à une jeune fille de 13 ans, victime de chantage sexuel par un individu résidant au Maroc. Nous avons mené les investigations nécessaires et nous avons pu identifier l'auteur et recueillir les cyber preuves qui l'ont incriminé.

Le Laboratoire a également traité 846 demandes d'expertises en 2021 sur divers supports numériques. Notre apport est devenu alors incontournable et on est présent dans quasi toutes les affaires judiciaires traitées au niveau de la Brigade Nationale de la Police Judiciaire.

Nous avons travaillé sur de grandes affaires qui ont ciblé des institutions bancaires ou des entreprises technologiques. Le maître-mot qui guide notre action est la rapidité, pour éviter que les traces ne disparaissent. C'est dans cet esprit que la communauté internationale a mis en place des points de contact entre les pays ayant ratifié la Convention de Budapest sur la cybercriminalité, opérationnels 24 heures sur 24 et 7 jours sur 7.

Bilan du Laboratoire d'analyse des traces numériques de la BNPJ-2021

Laboratoire d'Analyse des Traces Numériques de la BNPJ

846
expertises «digital forensic»

47
menaces sur Internet

22
affaires de cyberpédophilie

111
affaires

Ayant ratifié cette Convention en 2018, le Maroc a désigné deux points focaux: la DGSN, représentée par le Service central de lutte contre la criminalité liée aux nouvelles technologies relevant de la Direction de la Police Judiciaire; et la présidence du Ministère Public, représentée par le Pôle de suivi des affaires pénales et la protection des catégories spéciales. Dès qu'une urgence est signalée par un pays faisant partie de la Convention, peu importe le jour ou l'heure, le mécanisme est rapidement déclenché pour accélérer les démarches nécessaires ■

Les data analystes..

une plus-value dans l'élucidation des affaires criminelles les plus complexes

Noureddine NAJIH

Il est Commissaire de Police Principal et Chef du Service du Renseignement Criminel et d'Appui aux Enquêtes ***(SRCAE)*** *à l'Office National contre la Criminalité liée aux Nouvelles Technologies.*

Il a intégré les rangs de la DGSN en 2000 et fut affecté à la BNPJ la même année. Après plusieurs passages dans les divers offices de la BNPJ, ce gradé passionné, a travaillé dans les grandes affaires de trafic de drogues, de migration irrégulière ou de criminalité économique et financière qui ont marqué l'actualité marocaine. Chose qui lui a permis d'aiguiser et de perfectionner ses compétences. Après une année passée en tant qu'Officier de Liaison de la DGSN aux Pays-Bas en 2017, il fut désigné Chef de Service du reseignement criminel et d'appui aux enquêtes relevant de l'ONCLNT. Il a également bénéficié de formations pointues, dans le cadre de la coopération internationale, en matière des techniques d'enquête dans les affaires de trafic de drogues et représente la DGSN dans des commissions de haut niveau portant sur les efforts de lutte contre ce fléau. Un enquêteur aguerri qui met son savoir-faire et son esprit d'analyse, pour mettre fin aux activités criminelles les plus complexes et les plus sophistiquées.

Les grandes affaires criminelles ou celles revêtant une certaine sensibilité et complexité nécessitent une méthodologie bien organisée, ainsi que le recours à diverses ressources internes de l'institution et aussi externes. Ce genre d'affaire peut également drainer une masse importante de données, qu'il faudra structurer, analyser, recouper pour dégager des rapprochements et apporter ainsi, un appui aux enquêteurs en les orientant davantage.

C'est le travail que mène le Service du Renseignement Criminel et d'Appui aux Enquêtes, relevant de l'Office National contre la Criminalité Liée aux Nouvelles Technologies. Une entité composée de plusieurs analystes aguerris, qui examinent les détails les plus fins d'une procédure, y recherchent toutes les données d'importance, qui questionnent les bases de données de la DGSN et font appel à d'autres partenaires, pour rechercher toute information susceptible d'orienter l'enquêteur et conduire à l'identification des criminels.

Cette entité experte dispose d'outils techniques lui permettant d'analyser un grand flux d'information, de les trier, de ressortir les plus pertinentes et de faire des recoupements et des rapprochements, afin d'associer une personne à un endroit, un numéro téléphone à une activité, relier des personnes entre elles, etc.

Qu'est ce qui s'est réellement passé? Quel est le mode opératoire utilisé? Quand a été commise l'infraction? Où est-ce qu'elle a été commise ?

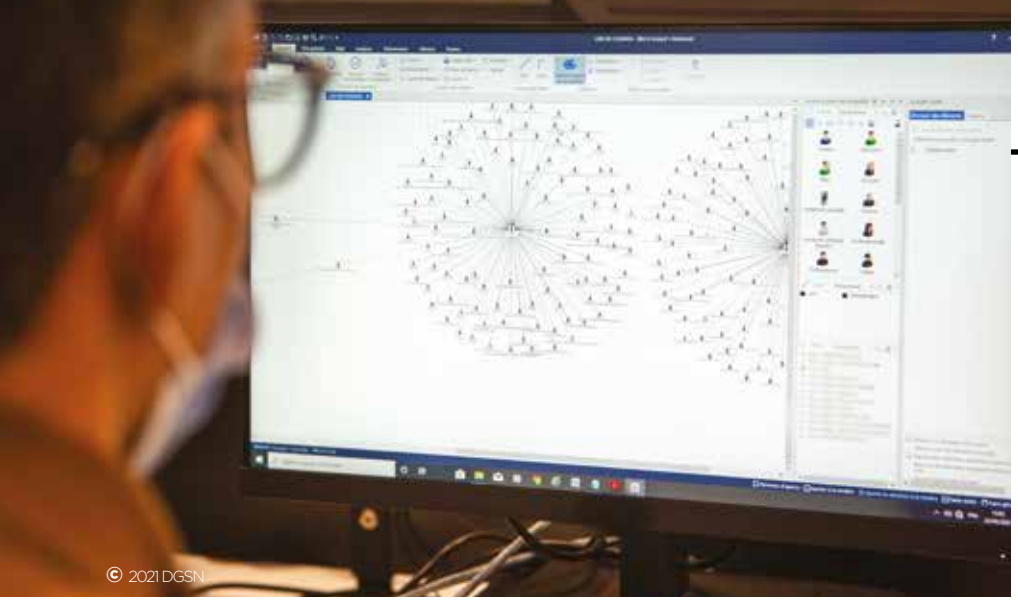
Quelques questions parmi tant d'autres que se posent ces analystes à l'esprit lucide et critique.

Le résultat est donné sous forme d'un schéma relationnel, comme il est appelé dans le jargon de ces analystes, qui donne une vue d'ensemble sur des liens jusque-là insoupçonnés par l'enquêteur, lui apportant ainsi un appui précieux et des pistes à explorer. Les résultats probants donnés par cette entité, en a fait un acteur clé dans les investigations criminelles, fortement sollicitée par les Officiers enquêteurs.

POLICE

En quoi consiste le travail du Service du Renseignement Criminel et d'Appui aux Enquêtes que vous dirigez ?

Le Service du renseignement criminel et d'appui aux enquêtes, que j'ai l'honneur de diriger, est une entité spécifique qui intervient dans quasi toutes les affaires qui parviennent à la BNPJ. Dans toute affaire complexe, les débuts sont toujours difficiles et les informations sont parfois éparpillées, voire contradictoires. L'enquêteur cherche le bout du fil et les pistes à explorer. Il dispose des fois d'un numéro de téléphone, ou juste d'une adresse e-mail ou d'une photo. C'est exactement à ce moment, qu'intervient notre action, pour essayer de lui donner un coup de main et faire avancer l'enquête. Au sein du service, nous sommes tous des enquêteurs et nous



avons bénéficié de formations très pointues pour devenir des analystes criminels.

Dès qu'on est saisi d'une affaire, on se réunit pour exposer toutes les informations disponibles. Toutes les informations recueillies sur le terrain par l'OPJ ou par le Laboratoire de l'analyse des traces numériques, débouchent au service. C'est à l'équipe de les examiner, de les décrypter et de les analyser.

Pour mener à bien notre travail, on fait appel aux bases de données mises à notre disposition, comme on peut formuler des réquisitions, sous la supervision du Parquet compétent, aux fournisseurs d'accès à Internet, aux opérateurs de téléphonie et même à d'autres partenaires privés.

Toutes les informations collectées sont analysées avec des outils dont nous disposons, permettant de faire des rapprochements qui sont schématisés dans une matrice analytique. On présente les résultats obtenus et éventuellement des hypothèses à l'enquêteur, qui vont orienter son action pour identifier le ou les auteurs, et procéder à l'arrestation et aux perquisitions.

Et notre travail ne s'arrête pas là, car après la perquisition, de nouveaux éléments et preuves seront saisis, sur lesquels le laboratoire d'analyses des traces numériques va effectuer des expertises, et au besoin nous solliciter pour reformuler des réquisitions et ainsi de suite. C'est un travail en cycle !!

Et si au cours de nos investigations, on tombe par exemple sur une adresse IP à l'étranger, nous faisons intervenir les canaux de coopération, via une commission rogatoire internationale, Interpol, le Bureau de Liaison Arabe, le point de contact de la Convention du Budapest ou les Officiers de Liaison accrédités au Maroc. Nous sommes en contact continu avec les OPJ et en temps réel, pour redéfinir les objectifs.

Nous donnons du sens à la masse d'informations qui risquent de noyer l'OPJ et de lui faire perdre un temps précieux. Et dans notre travail, le temps n'est jamais notre allié. Quand on travaille sur une affaire importante et sensible, on reste mobilisé non-stop. On y met toute notre énergie et nos efforts. Aujourd'hui l'apport de l'analyse du renseignement criminel n'est plus à démontrer, car il a permis de solutionner beaucoup de grandes affaires criminelles.

Vous avez parlé de partenaires, pouvez-vous développer un peu plus ?

Vous savez, la nature des affaires confiées à la BNPJ sont très complexes certes, mais également très diverses, et nécessitent d'avoir des informations que détiennent plusieurs institutions publiques et privées. Ces informations sont des fois déterminantes pour l'aboutissement de l'affaire, surtout quand il s'agit d'affaires de blanchiment d'argent, de terrorisme, de piratage informatique ou de pédopornographie.

Les forces de sécurité ne peuvent alors rester les mains nouées sans rien faire. C'est pour cela qu'en plus des mécanismes de coopération internationale, nous avons développé des partenariats avec plusieurs institutions publiques et privées au niveau national, telles que les banques, les agences de transfert d'argent, les assurances, l'Agence Nationale de la Conservation Foncière, du Cadastre et de la Cartographie et bien d'autres. Nous faisons appel à ces entités par le biais de réquisitions judiciaires, ayant reçu le consentement du parquet compétent.

La sécurité est globale et engage toutes les composantes de la société tant les individus que les institutions publiques et privées. Grâce à cette fructueuse collaboration, nous arrivons à mettre fin aux activités criminelles les plus complexes.

Quel a été votre bilan au cours de l'année 2021 ?

Notre activité connaît une hausse exponentielle d'année en année. Pour l'année 2021, nous avons envoyé et traité 11.400 réquisitions à divers partenaires contre 2.232 en 2018. Cela étant et au-delà de ce chiffre, c'est l'analyse des données qui nous ont été transmises, qui est chronophage, car il faut regarder les informations avec minutie, les analyser et les présenter à l'enquêteur de manière simplifiée et facilement saisissable.

Grâce à ce travail, nous avons pu solutionner des affaires de phishing et de ransomware qui ont touché plusieurs établissements bancaires et des entreprises marocaines.

Au cours de cette année, la BNPJ a été saisie par les autorités judiciaires d'une plainte formulée par une société internationale, qui a été victime de phishing de manière récurrente. Le mode opératoire adopté se basait sur l'envoi d'e-mails contenant des liens suspects, qui une fois téléchargés, le cybercriminel s'accapare alors de leurs données personnelles et des mots de passe utilisés pour l'accès au système d'information de cette entreprise.

L'Office avec ses différentes composantes a mené l'enquête et a pu arriver à l'identité du cybercriminel et son adresse, avec le concours du Laboratoire d'analyses des traces numériques. La perquisition effectuée à son domicile a permis la saisie de matériels informatiques, qui ont été expertisés, ayant permis de trouver les preuves de la commission de ces infractions et ce depuis 2019.

Une autre affaire me vient à l'esprit, c'est l'affaire d'un cybermalfaiteur qui utilisait le pseudonyme « Dr HEX », recherché par Interpol, pour intrusion et piratage de cartes bancaires et données à caractère personnel à l'échelle mondiale, et ce, depuis plus d'une dizaine d'années. Il avait procédé au défacement de sites Web en modifiant la présentation et le contenu d'institutions bancaires et d'entreprises. Ce cybercriminel a également utilisé les réseaux sociaux et forums pour vendre des kits d'hameçonnage. Les investigations menées par l'Office et les expertises effectuées par le Laboratoire de Traces Numériques, ont permis de mettre fin à l'activité criminelle de ce cyber malfaiteur ■

LA DÉSINFORMATION EN LIGNE..

«nouveau» fléau des sociétés modernes

Si la rumeur n'est pas un phénomène nouveau, elle se trouve néanmoins, amplifiée et démultipliée par le Web, les réseaux sociaux et les plateformes de discussion instantanée « chat ». En effet, si le web sémantique et les réseaux sociaux ont apporté de nouveaux modes de communication, d'échange et de débats, ils sont également devenus le lieu privilégié de fausses publications de tous genres, qui se trouvent commentées, relayées et partagées à outrance, se propageant tellement vite, causant un impact économique, financier, d'image et de notoriété. La désinformation s'immisce dans notre quotidien, manipule nos opinions et aggrave même les tensions sociétales au point de créer une déstabilisation et un manque de confiance dans les efforts des institutions. Un autre phénomène des plus inquiétants, est le deepfake, ces algorithmes qui font usage de la voix et de l'image, rien que cela !! Derrière ces avalanches de fausses informations, des Etats, des entreprises, des organisations criminelles ou extrémistes et même de simples individus. Et la désinformation n'épargne aucun sujet, santé publique, politique, sécurité, environnement, image et notoriété, etc. Si les motivations sont diverses, le danger réside dans les théories complotistes, qui cherchent à manipuler l'opinion publique, à déstabiliser et à endoctriner les personnes, à des fins politiques, idéologiques ou autres. Au niveau mondial, les Etats, bien conscients de la gravité de cette nouvelle menace et de ses multiples impacts et répercussions, ont fait de la lutte contre la propagation de la désinformation, un axe majeur de leur stratégie d'action en matière de réglementation, de fact-checking, de solutions technologiques de détection en ligne, mais aussi de sensibilisation et d'éducation. En effet, sensibiliser le public depuis le jeune âge, ultime récepteur de l'information, développer des réflexes de base pour ne pas croire tout ce qu'on voit circuler en ligne et d'être en mesure de décoder le faux du vrai, sont devenues des actions importantes à considérer, pour ne pas être un acteur qui alimente la rumeur. Fort heureusement, l'essor de nouvelles technologies, dont notamment l'intelligence artificielle, pourrait éventuellement constituer un bon outil pour faire la part des choses et faire face à l'effet boule de neige généré par la désinformation.

Le 25 novembre 2021, la Revue de Police a assisté à une conférence, dans le cadre du cycle **« Morocco21 »**, lancé par News Africa Holding (NCA Holding) à Casablanca, portant sur la cybersécurité et les fake news, animée par **M. Dan BRAHMY**, expert international et co-fondateur d'une start-up israélienne « CYABRA », spécialisée dans la lutte contre les fake news et plus spécialement l'analyse de l'effet boule de neige généré par les fake news et les deepfakes, et a saisi cette opportunité pour recueillir son avis sur le phénomène de la désinformation en ligne..

« Un mensonge peut faire le tour de la terre, le temps que la vérité mette ses chaussures »
Mark TWAIN

Qui est DAN BRAHMY ?

Permettez-moi tout d'abord de vous exprimer ma grande joie d'être ici au Maroc avec lequel j'ai un lien particulier, puisque mes grands-parents sont d'origine marocaine et tunisienne. Je suis né et j'ai grandi à Paris, jusqu'à l'âge de 15 ans, d'où je suis parti vers Israël. Je suis marié et j'ai un petit garçon d'un an. J'ai commencé ma carrière professionnelle dans une start-up technologique, ensuite chez Google, en tant commercial pour la Région Europe, Moyen-Orient et Afrique, et enfin chez Deloitte Digital en tant que chargé de la stratégie et des ventes. Depuis 2018, j'occupe le poste de président-directeur général de « CYABRA », une start-up «tech» que j'ai co-fondé avec d'autres partenaires, spécialisée en cybersécurité et lutte contre la désinformation.

Que propose votre start-up pour lutter contre la désinformation ?

« CYABRA » est une start-up de développement de solutions technologiques en matière de lutte contre les fake news et les deepfakes.

Nous fournissons également des solutions pour être en mesure d'analyser la prolifération de ces menaces en ligne et leur impact, qu'on appelle « l'effet boule de neige » ou avalanche, ainsi que l'authenticité des acteurs et du contenu.

Enfin, l'étendue de plateformes logicielles de fourniture de services « SaaS », est unique, compétitive et avantageuse, comparativement à d'autres solutions du genre existant sur le marché. Notre solution offre une interface très simplifiée, qui a été utilisée par de grandes entreprises financières et agences gouvernementales à travers le Monde, dont notamment, le Département d'Etat Américain, Warner et l'agence de publicité TBWA.

La désinformation est devenue à l'ère d'internet une réelle préoccupation. Quelles technologies sont mises en œuvre pour repérer les fake news ?

En effet, la désinformation accélérée par les plateformes de médias sociaux, est devenue une préoccupation majeure au niveau mondial. Pour développer des solutions de détection et de riposte efficaces, il est important avant toute chose,

de comprendre comment est créée la désinformation et comment elle est diffusée. C'est très important.

Pour lutter contre cette menace, des conglomérats de médias, des agences gouvernementales et même des organisations non gouvernementales à travers le monde, ont mis en place des méthodologies pour détecter et lutter contre les fake news, qu'on peut catégoriser en analyses manuelles et analyses par outils technologiques.

La majorité des technologies disponibles actuellement sur le marché se basent sur les analyses manuelles, qui sont ardues, compte tenu du volume important d'informations diffusées à chaque instant sur Internet et les réseaux sociaux, ainsi que la rapidité de leur propagation.

C'est pour cela que des entreprises technologiques, comme la notre «Cyabra», ont déployé beaucoup d'efforts et engagé des moyens financiers colossaux, en matière de recherche et de développement, pour mettre en place des solutions automatisées et évolutives, afin d'accroître la capacité de détection de la désinformation en ligne et les avalanches qui en résultent. Maintenant, le plus challengeant dans une solution automatisée, c'est la catégorisation du contenu écrit de manière automatisée, évolutive et sans biais, c'est-à-dire une vérification efficace des faits. L'intelligence artificielle pourrait apporter une plus-value appréciable pour détecter les informations et les catégoriser et peut donc devenir un outil de «fact-checking » par excellence.

Quel est l'impact de la désinformation?

L'industrie de la désinformation et des fake news, qui représente une sous-catégorie des menaces de cybersécurité, a causé des pertes financières colossales estimées à de plus de 80 millions de Dollars US par an (données de 2019), et ira certainement crescendo.

L'essor des plateformes de médias sociaux et leurs moteurs de propagande intégrés sont en faveur de telles menaces, car elles créent d'immenses profits financiers. Et les exemples d'illustration sont nombreux.

La désinformation a coûté beaucoup d'argent à plusieurs entreprises internationales cotées dans la bourse. En 2016, la publication sur Twitter d'une fausse information sur le PDG de PEPSICO a entraîné une perte de 10% de son chiffre d'affaires. Il en est de même pour Starbucks et leur programme de fidélité. Le «pump & dump », ces techniques de manipulation de marché et escroqueries à la bourse, qui visent de grandes entreprises sur le marché américain. Mais au-delà des aspects liés aux gains financiers, il y a d'autres motivations et d'autres impacts beaucoup plus graves, qui sont politiques, comme la manipulation des élections. Et ce n'est que la partie visible de l'iceberg d'après nos analyses des menaces.

Qui sont les acteurs de la désinformation?

Les acteurs sont divers et nombreux et cachent bien leurs motivations et leurs agendas, et ce, qu'il s'agisse d'une motivation financière, politique, gouvernementale, environnementale ou même pour une raison d'ennui ou d'orgueil. Les possibilités sont infinies, mais il semble qu'une grande majorité de menaces de désinformation peuvent être classées comme des activités dirigées par des Etats ou des entreprises de relations publiques (lorsque les entreprises paient pour attaquer la renommée ou falsifient le statut négatif d'autres firmes).

Nous pouvons aussi, tous devenir acteurs potentiels de la désinformation, juste en cliquant sur un « like », en commentant ou en repartageant l'information, sans être sûr de sa véracité.

Il y en a aussi qui en font un jeu, tels les trolls ou les bots, d'autres un business. Mais les plus dangereux sont, sans aucun doute, ceux qui sont animés d'une idéologie ou par des théories complotistes, cherchant à manipuler l'opinion publique, à déstabiliser et à endoctriner.

Mais, il faut préciser qu'il est très difficile de retracer une attaque, et cela étant dû à la nature insidieuse et mystérieuse, qui se cache derrière les murs des plateformes des médias sociaux.

Le deepfake, la vérité alternative, etc. sont de nouveaux phénomènes préoccupants. Comment, selon-vous, lutter contre ces menaces ?

La réponse est tout simplement: ***S'y préparer***. En premier lieu, il faudrait suivre de près les menaces potentielles et ne pas se contenter d'êtreun simple spectateur. Deuxièmement, il est important de construire un fondement basé sur une stratégie de remédiation et de contre-mesure. Il faut comprendre comment ont été orchestrées ces avalanches de fake news et qui en est à l'origine. Troisièmement, il est important d'établir des départements de R&D pour développer ou soutenir/analyser des remèdes contre de telles menaces. Enfin, tisser des partenariats avec d'autres acteurs impliqués dans la lutte contre la désinformation.

Devant cette apparente explosion des fausses nouvelles qui semble caractériser les dernières années, comment aider les citoyens à démêler le vrai du faux et vérifier une information ?

Face à ces avalanches d'informations qui inondent notre quotidien et qui influencent nos opinions, la sensibilisation et l'éducation sont la clé. Certains pays ont commencé à lancer des programmes de sensibilisation et d'éducation, pour être en mesure d'identifier la désinformation en ligne, en particulier pour les jeunes, qui sont les plus exposés et les plus vulnérables.

Pour conclure, chacun à son niveau peut contribuer à la lutte contre la désinformation en ligne, par l'adoption de réflexes simples, avant de cliquer, commenter ou partager, qui ne prendront que 30 secondes. Prendre juste le temps de lire et de se poser la question, est-ce que c'est vrai? Ensuite, prendre quelques secondes pour lire les commentaires, ça peut donner une idée sur les intentions et enfin vérifier l'authenticité de la source, est-ce une source fiable et reconnue ?

30 secondes suffisent, pour ne pas être un acteur de la désinformation en ligne!!