CyberSud
Coopération en matière de lutte contre
la cybercriminalité dans le Voisinage Sud

Version 30 décembre 2018

Rapport de situation initiale

sur les capacités des unités de lutte contre la cybercriminalité et des laboratoires scientifiques au Maroc

établi dans le cadre du projet CyberSud

Financé
par l'Union européenne
et le Conseil de l'Europe

UNION EUROPÉENNE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Mis en œuvre
par le Conseil de l'Europe

Liste des abréviations

ANRT	**Agence Nationale de Réglementation des Télécommunications**
CERT	Computer Emergency Response Team
CMI	Centre Monétique Interbancaire
CSSSI	Comité Stratégique de la Sécurité des Systèmes d'Information
DGSN	Direction Générale de la Sûreté Nationale
DGSSI	Direction Générale de la Sécurité des Système d'Information
DPJ	Direction de la Police Judiciaire
DST	Direction de la Surveillance du Territoire
FSI	Fournisseur de Services Internet
IoT	Internet of Things (Internet des Objets)
LCTN	Laboratoire Central des Traces Numériques
LRATN	Laboratoire Régional d'Analyse des Traces Numériques
PIC	Protection des Infrastructures Critiques
PAC	Pièces à conviction
POC	Point of Contact (Point de contact)
SLCNT	Service de Lutte contre la Cybercriminalité liée aux Nouvelles Technologies
SSI	Sécurité des Systèmes d'Information
SPOC	Single Point of Contact (Point de contact unique)
STAD	Système de Traitement Automatisé de Données
TIC	Technologies de l'Information et de la Communication
VPN	Virtual Private Network

TABLE DES MATIERES

1 Introduction 4
1.1 Description du projet CyberSouth (CyberSud) 4
1.2 L'objet du rapport 4
1.3 La collecte d'information 5
2 Vu d'ensemble de la digitalisation de la société marocaine 6
2.1 Les usages du numérique au Maroc 6
2.2 Les avancées consacrées en matière de cybersécurité : le plan Maroc numérique 7
3 La stratégie de lutte contre la cybercriminalité de la DGSN 7
3.1 Un cadre juridique renforcé 8
3.2 Des mesures organisationnelles et mesures logistiques 8
3.3 Un investissement dans les ressources humaines 9
3.4 Une ouverture sur le partenariat pour la prévention 9
4 Les structures de la lutte contre la cybercriminalité au sein de la DGSN 9
4.1 Les structures centrales 9
4.2 Structures au niveau régional 10
4.2.1 Vue d'ensemble 10
4.2.2 Laboratoire Régional d'Analyse des Traces Numériques (LRATN) de Marrakech 10
5 Formation 10
6 Conclusions et recommandations 11
6.1 Conclusions 11
6.2 Recommandations 11

1 Introduction

1.1 Description du projet CyberSouth (CyberSud)[1]

Les pays du Voisinage Sud, à l'instar d'autres pays dans le monde, sont confrontés aux difficultés liées à la dépendance croissante de nos sociétés aux technologies de l'information et de la communication, et notamment au phénomène de la cybercriminalité. Il est donc essentiel pour ces pays de renforcer leurs capacités institutionnelles afin de répondre aux défis de la cybercriminalité sur le plan national, régional et international. Par le biais du projet CyberSud, l'Union européenne et le Conseil de l'Europe, en coopération avec d'autres partenaires, soutiendront cet effort de lutte sur la base d'outils et d'instruments existant, y compris la Convention de Budapest sur la Cybercriminalité.

OBJECTIF ET RESULTATS ATTENDUS DU PROJET

Objectif : Renforcer la législation et les capacités institutionnelles de lutte contre la cybercriminalité et d'utilisation des preuves électroniques dans la région du Voisinage Sud en conformité avec les exigences relatives aux droits de l'Homme et à l'Etat de Droit.

Résultat 1 - Cadres de droit pénal renforcés conformément aux dispositions de la Convention de Budapest sur la cybercriminalité, y compris la règle de respect des sauvegardes prévue par le droit interne (article 15).

Résultat 2 – Renforcement des services de police et de poursuites spécialisés et de l'ATT et renforcement de la coopération interservices.

Résultat 3 - Standardisation de la formation des membres du système judiciaire à la lutte contre la cybercriminalité et au traitement des preuves électroniques.

Résultat 4 - Les points de contact 24/7 sont opérationnels (au niveau du parquet et /ou de la police) pour une coopération internationale plus efficace en matière de cybercriminalité et de preuve électronique.

Résultat 5 - Les stratégies prioritaires en cybercriminalité et preuve électronique sont identifiées.

1.2 L'objet du rapport

L'objet du présent rapport est de faire un état des lieux de la situation en matière de cybercriminalité et de preuve électronique au Maroc par un recensement :

- **de l'état de la menace,**
- **des institutions responsables,**
- **de la formation,**
- **et de la coopération internationale.**

Le succès d'un projet dépend d'une multiplicité de paramètres ainsi que de l'engagement de tous les acteurs, c'est pourquoi le rapport conclut par une série de recommandations à destination des autorités marocaines et également au Conseil de l'Europe.

[1]La dénomination exacte du projet selon l'accord de délégation conclu entre le Conseil de l'Europe et l'Union européenne (ENI/2017/385-202) est Cybercrime@South

1.3 La collecte d'information

Les 10 et 11 décembre 2019, les projets CyberSud et CT MENA (sur le contre-terrorisme dans la région Afrique du Nord Moyen Orient), ont mené conjointement une visite d'études afin d'établir les capacités de lutte contre la cybercriminalité et le traitement de la preuve électronique par la Direction Générale de la Sûreté Nationale (DGSN) du Royaume du Maroc au niveau central à Rabat et au niveau régional à Marrakech. L'objet des visites étaient d'identifier les besoins en matière de formation, de confirmer la connaissance des structures des unités spécialisées, leurs compétences en matière d'enquêtes et de procédures dans le domaine de la coopération nationale et internationale.

La délégation était composée de :

- Serge Houtain, Commissaire, Chef de Service de l'Unité Régionale de Cybercriminalité à Mons, Police Judiciaire Fédérale, Belgique
- Valérie Maldonado, Commissaire divisionnaire, Sous-direction de la lutte contre la cybercriminalité
- Etienne Dubern, expert projet CT MENA
- Ionut Stoica, chargé de projet expérimenté, projet CyberSud, Conseil de l'Europe.

2 Vu d'ensemble de la digitalisation de la société marocaine

2.1 Les usages du numérique au Maroc

Fin 2017, le Maroc comptait 47 millions d'abonnés en téléphonie mobile soit un pourcentage d'équipement de 123%.

S'agissant d'internet, 22,2 millions d'internautes ont été recensés avec une forte évolution à partir de 2015 qui poursuit une accélération remarquable. Le réseau le plus cité est très majoritairement FACEBOOK, avec 16 millions d'abonnés en 2017 suivi de plus loin par la messagerie Instagram puis par Google et Twitter.

Les grands opérateurs télécoms sont : Maroc télécom, Orange télécom et INWI.

De manière complémentaire, la revue « le Temps »[2] rapporte dans une enquête réalisée par Kaspersky Lab en partenariat avec le cabinet marocain AVERTY d'études de marché et de sondages d'opinion, que près de 9 marocains sur 10 sont attirés par les métiers de la cybersécurité. 85 % d'entre eux indiquent que la sécurité informatique est un métier d'avenir.

Par ailleurs, de nombreuses initiatives sont prises pour favoriser la montée en puissance des sociétés de service dédiées aux nouvelles technologies, au sens large du terme : INWI , opérateur marocain a décroché le grand prix Smart City Africa, avec son projet de déploiement d'un réseau WiFi très haut débit dans le tramway de Casablanca. Il a ainsi permis aux 125,000 utilisateurs quotidiens du tramway de bénéficier d'une connexion gratuite et stabilisée.

La platforme numerique JUMIA est devenue au Maroc une véritable market-place, plus de trois millions de personnes étaient en effet attendues au « black friday » de novembre 2018.

Le centre monétique interbancaire (CMI) a lancé une grande opération visant à favoriser les paiements électroniques au Maroc. Le CMI s'engage en effet pour le développement des paiements électroniques et la dématérialisation des transactions commerciales au Maroc.

Enfin la banque nationale du Maroc (bank Al-Magghrib) et l'agence nationale de réglementation des télécommunications (ANRT) soutiennent le projet du paiement mobile : le téléphone porte-monnaie pour tous, cf. revue « Le Reporter » 2 de décembre 2018[3]). Il s'agit d'un moyen de paiement nouvelle génération qui va permettre de réaliser de manière électronique et dématérialisée, des opérations de paiement entre commerçants, de transferts d'argent de personne à personne, ainsi que des opérations de retrait et de dépôt d'espèces.

Ces entités institutionnelles ont en effet misé sur le taux de pénétration de la téléphonie mobile qui atteint les 123 %. Un taux qui double celui de la bancarisation qui n'atteint aujourd'hui que 65 %. Les échanges au Maroc sont encore largement dominés par les paiements en espèces. Il s'agit là de réduire la circulation du cash et de développer l'inclusion financière.

[2] Revue « LE TEMPS » n° 437 du 7 au 13 décembre 2018
[3] Revue « le reporter » n°932 du 06 au 13 décembre 2018,

2.2 Les avancées consacrées en matière de cybersécurité : le plan Maroc numérique

Le plan numérique du Maroc comporte quatre axes majeurs :

- Un renforcement du cadre législatif dans lequel s'inscrivent les actions de la DGSSI (qui dépend de la Défense nationale). La DGSSI est plus particulièrement en charge des audits SSI, des process de veille et de détection des attaques et de lancement des alertes. Elle apporte une assistance technique aux administrations et aux organismes publics. Le CERT Marocain a été créé quant à lui en 2011.
- L'accompagnement de la transformation sociale face aux nouvelles technologies,
- Favoriser la productivité des petites et moyennes entreprises dans l'environnement numérique et digital.
- Encourager le développement de la filière industrielle tournée vers les nouvelles technologies.

Agence de Développement du Digital (ADD), a été créée en vertu de la loi N°61.16 publiée au bulletin officiel n°2-17-764 du 14 septembre 2017.

Cf la revue de Police publiée par la DGSN3 n°29 : les enjeux de la sécurité de l'information ont été clairement identifiés. Raison pour laquelle, un projet de mise en place d'un Système de Management de la Sécurité du Système d'Information (SMSI) a été adopté.

En outre, la protection des infrastructures du Maroc est intégrée dans une nouvelle approche de sécurité (cf. revue susvisée) :

- Le cadre législatif et institutionnel de la PIC (protection des infrastructures critiques) au Maroc comprend une référence principale en la matière, le décret du 22 mars 2016 fixant le dispositif de protection des systèmes d'information sensible, des infrastructures d'importance vitale et l'identification des risques majeurs. Le texte a été préparé par l'administration de la Défense (DGSSI).

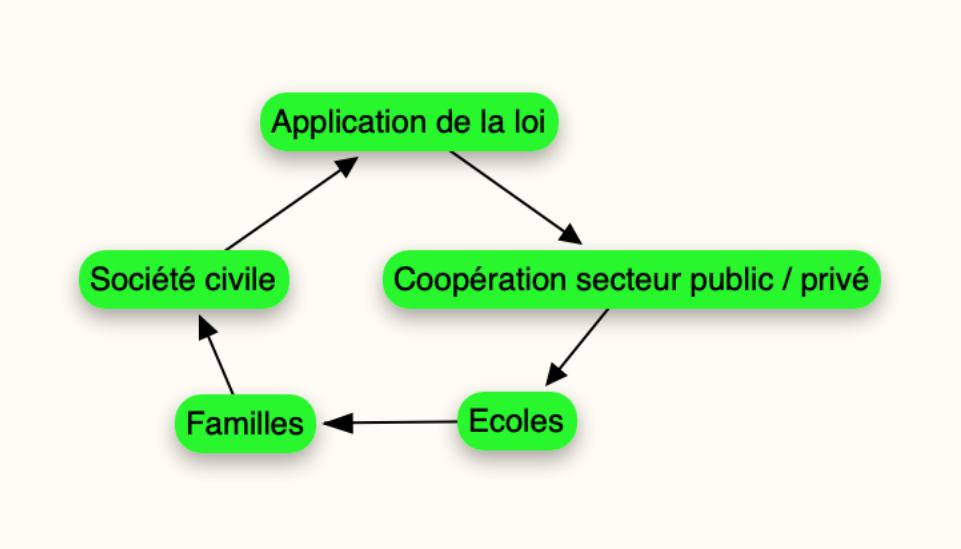
- La direction générale de la sécurité des systèmes d'information est l'autorité compétente auprès de laquelle les exploitants et propriétaires des infrastructures vitales sont tenues de communiquer la liste des systèmes d'information sensibles dont ils disposent. Les dispositions s'appliquent ainsi aux administrations, établissements entreprises publiques et organismes disposant d'un agrément ou d'une licence de l'état pour exercer une activité réglementée.

- Par ailleurs un décret du 21.09.2011, consacre la création du comité stratégique de la SSI chargé d'établir les orientations stratégiques dans le domaine de la SSI pour garantir la sécurité et l'intégrité des infrastructures marocaines et statuer sur les projets de loi et des normes relatifs à la SSI.

3 La stratégie de lutte contre la cybercriminalité de la DGSN

La DGSN **dispose clairement d'une vision stratégique globale à long terme.**

Cette **stratégie** est **intégrée** et **intégrale**, tant sur le plan organisationnel que du point de vue de la gestion des ressources humaines, et elle s'applique tant au niveau central qu'au niveau régional.



Pour la DGSN, la communication et le dialogue sont fondamentaux, et même vitaux, tant entre les différents services qu'avec les FSI, le secteur public, le secteur privé, les écoles (sensibilisation des enfants aux dangers d'internet), l'éducation familiale, et sans oublier les apports de la société civile.

La DGSN a très bien développé, au sein de sa Direction de la Police Judiciaire, des structures pour contrer le phénomène de la cybercriminalité.

L'objectif du plan stratégique est de doter l'ensemble des préfectures du Royaume de moyens adéquats répondant aux **normes internationales** en matière de lutte contre la cybercriminalité.

Cette stratégie globale est déclinée à plusieurs niveaux :

3.1 Un cadre juridique renforcé

Le cadre juridique et règlementaire a été mis à jour pour la prise en compte de la protection des données personnelles par exemple, ou encore par la mise en place d'un dispositif législatif dédié à la répression des atteintes aux STAD, une loi sur le terrorisme, la prise en compte de la propriété intellectuelle et un statut juridique précisé pour les transactions électroniques.

La coopération internationale ou régionale s'appuie essentiellement sur la cooperation via Interpol, la convention de Budapest et le bilateral

3.2 Des mesures organisationnelles et mesures logistiques

A Rabat, le service de lutte contre la cybercriminalité liée aux nouvelles technologies (le SLCNT) prend en compte la gestion des points de contacts pour la coopération internationale, en binôme avec la Présidence du Ministère publique.

S'agissant plus spécifiquement de la mise en place du point de contact 24/7 qui permet notamment d'effectuer ou de solliciter directement auprès des autres points de contacts des états signataires de la Convention de Budapest, et en urgence, les demandes de gel de données techniques, la Présidence du Ministère publique a organisé un séminaire de formation et de concertation à Marrakech au mois de décembre 2018 qui a réuni 90 procureurs, 40 magistrats du siège, 30 officiers de la lutte contre la cybercriminalité, le SLCNT, la Gendarmerie Royale et la Défense. C'est à l'occasion de ce rassemblement qu'ont été élaborées les modalités de fonctionnement de ce point de contact qui requiert pour chaque demande, l'aval du Parquet (autorité judiciaire). Une adresse email dédiée a été créée et un fonctionnement continu a été prévu.

Le laboratoire central du Digital Forensic relève de l'Institut des Sciences Forensiques de la Sûreté Nationale.

En 2018, un Office National de lute contre la Criminalité liée aux Nouvelles Technologies a été créé au niveau de la Brigade Nationale de la Police Judiciaire.

Plus de détail sur l'organisation est fournie au paragraphe 5.

3.3 Un investissement dans les ressources humaines

–

– Depuis 2005, des recrutements de profils spécialisés ont été effectués : ingénieurs d'État informatiques et techniciens.

– Les différentes équipes spécialisées sont composées d'ingénieurs, de techniciens spécialisés, d'enquêteurs, mais aussi de juristes et d'analystes à différents niveaux.
Les formations aux nouvelles technologies sont intégrées dans l'ensemble des niveaux de grades de la police : gardiens de la paix (une session de formation de 8 heures est consacrée), les officiers et les commissaires (3 jours sont proposés). Les niveaux de formation sont progressifs : sensibilisation, et cursus plus spécialisés. Elles comportent une partie réservée à la connaissance des infractions pénales cyber/des présentations des cas pratiques en association avec le laboratoire digital forensic. Ces formations sont déployées au sein de l'Institut Royal de police de Kenitra.

–

– Des outils dédiés sont mis à disposition des enquêteurs : connexion internet dédiée, des canevas d'audition et d'intervention forensic simplifiés.

3.4 Une ouverture sur le partenariat pour la prévention

Les écoles, famille et société civile, constituent des publics exprimant des besoins face aux menaces cyber. Des supports pédagogiques sur les modes opérateurs des principales menaces cyber ont été réalisées pour la sensibilisation du public. Des interventions sont également réalisées sur les dangers de l'internet au sein des écoles primaires, collèges et lycées. La DGSN organise, chaque année, ses journées portes ouvertes, qui s'étalent sur cinq jour, aveu stand dédié à la cybercriminalité est instauré, comprenant des ateliers et des tables rondes autour de la lutte contre la cybercriminalité. Ces journées ont remporté un franc succès, les attentes du public étant très importantes.

4 Les structures de la lutte contre la cybercriminalité au sein de la DGSN

4.1 Les structures centrales

Au **niveau central**, la structure de lutte contre la cybercriminalité comprend :

– Le Service central de lutte contre la criminalité liée aux technologies de l'information et de la communication (SLCNT)
– Le Laboratoire Central des Traces Numériques (LCTN) qui se charge de réaliser des expertises sur les supports numériques saisis par les services de police au niveau national.
– Office National de lutte contre les infractions liées aux technologies de l'information et de la communication

4.2 Structures au niveau régional

4.2.1 Vue d'ensemble

La DGSN dispose de **6 laboratoires forensiques** spécialisés répartis dans le pays, soit à :

- Rabat (laboratoire central),
- Un Laboratoire à la Brigade Nationale de la Police Judiciaire Marrakech,
- Fès,
- Casablanca,
- Laâyoune.
-

D'autre part, **29 brigades spécialisées** dans la lutte contre la cybercriminalité sont réparties géographiquement dans le pays.
Quatre de ces brigades disposent d'un laboratoire (Casablanca, Fès, Marrakech, et Laâyoune).

4.2.2 Laboratoire Régional d'Analyse des Traces Numériques (LRATN) de Marrakech

Le LRATN a été créé en décembre 2012 et ses missions consistent en la collecte et l'analyse des supports informatiques.

La visite a été l'occasion de comprendre la chaine de traitement des pièces à conviction (cf. « chain of custody »). Celle-ci est classique et correcte par rapports aux standards internationaux.

Les logiciels principaux utilisés sont EnCase, FTK Imager, IEF, UFED. Les rapports rédigés à la suite d'une analyse reprennent les processus utilisés ainsi que les éléments pertinents.

Les participants marocains insistent sur la nécessité de rédiger l'inventaire des PAC, la traçabilité, le double-encodage (papier et informatique).
Il existe un principe (toutefois non obligatoire) de double-signature du rapport d'analyse, soit une analyse effectuée par un opérateur et vérifiée par un second opérateur.

Les difficultés. A l'instar des autres pays/services spécialisés, les participants font part des difficultés ou blocages par rapport à l'exercice de leurs fonctions spécialisées, soit :

- la collecte de données et l'analyse pour les IoT ;
- les recherches dans le Cloud ;
- outils forensiques d'extraction (smartphones verrouillés, drones, …) ;

5 Formation

Des formations thématiques ont été mises en place. L'objectif est d'augmenter la sensibilisation aux délits faisant appel aux TIC et d'augmenter le degré de vigilance en la matière.

Les formations sont composées de « packs » différenciés en fonction du grade (ex. Gardien de la Paix, Inspecteur, Officier et Commissaire).
La formation de base de chaque policier (peu importe l'affectation) comprend un volet cybercriminalité.

6 Conclusions et recommandations

6.1 Conclusions

La DGSN présente une stratégie de lutte contre la cybercriminalité complète, au sein de laquelle les enjeux de la prise en compte de cette nouvelle délinquance sont parfaitement identifiés. Les présentations réservées aux experts et au représentant du Conseil de l'Europe ont été effectuées autant à Rabat qu'à Marrakech, dans un esprit d'ouverture et de modernité.

Il s'agit d'une organisation structurée, disposant des capacités logistiques, humaines, et d'une très bonne vision du phénomène cybercriminalité. La DGSN a une réelle volonté d'offrir une réaction efficace dans la lutte contre la cybercriminalité, et d'être présente et réactive sur l'ensemble du territoire national.

Les demandes de formations sur des sujets spécifiques sont les mêmes qu'ailleurs et concernent les difficultés d'investigations inhérentes à l'évolution permanente de la technologie.

6.2 Recommandations

- Un suivi de la mise en place des unités territoriales cyber serait pertinent, accompagné d'un plan de formation élargi à ces acteurs territoriaux (principe d'une formation basique pour les premiers intervenants cyber) ;

- Un rapport annuel de l'état de la menace cyber au sens large serait judicieux : cette étude devrait être partagée avec les autres ministères concernés par les nouvelles technologies, particulièrement avec le Ministère du Commerce, de l'Investissement, de l'Industrie et de l'Economie Numérique et l'Agence Nationale de Réglementation des Télécommunications (ANRT), le secteur monétique ;

- Un suivi des réformes législatives qui devraient être engagées pour l'adoption de moyens spéciaux d'enquête adaptés à l'investigation numérique (enquête sous-pseudo, téléperquisition) paraît opportun ;

- Des pistes de réflexion pourraient être engagées pour une meilleure prise en compte des « contentieux de masse » cyber :

    - les escroqueries sur internet par exemple,
    - les extractions de premier niveau, automatisées et sécurisées des données contenues dans les supports mobiles (particulièrement les téléphones mobiles) .