

ROYAUME DU MAROC
ADMINISTRATION DE
LA DEFENSE NATIONALE



LA STRATÉGIE NATIONALE DE CYBERSÉCURITÉ 2030



DIRECTION GÉNÉRALE DE LA SÉCURITÉ
DES SYSTÈMES D'INFORMATION



SA MAJESTÉ LE ROI MOHAMMED VI QUE DIEU L'ASSISTE

SOMMAIRE



5 RESUME EXECUTIF

9 INTRODUCTION

11 VISION

13 LA CYBERSECURITE AU MAROC

13 Paysage des menaces et cyber risques

13 Acquis de la Stratégie Nationale en matière de cybersécurité 2012

14 Cadre institutionnel

16 Cadre juridique et normatif national propre à la cybersécurité

19 PILIERS STRATEGIQUES

20 Gouvernance nationale de la cybersécurité : cadre institutionnel et juridique

24 Sécurité et résilience du cyberspace national

30 Développement des capacités et sensibilisation

38 Coopération régionale et internationale

43 SUIVI ET EVALUATION





RESUME EXECUTIF

Les nouvelles technologies de l'information et de la communication s'imposent comme un véritable levier de développement économique et social. Touchant tous les domaines et affectant tous les aspects de la vie des citoyens, entreprises et administrations, la digitalisation offre des perspectives infinies mais donne naissance aussi à des défis en termes de cybersécurité.

Pour répondre à ces défis et tirer en même temps profit des opportunités offertes par l'évolution des technologies de l'information, le Maroc a toujours choisi d'inscrire son action en matière de cybersécurité dans le cadre d'une démarche stratégique. Sous la conduite éclairée de **Sa Majesté Le Roi**, que Dieu l'Assiste, les efforts déployés dans le cadre de la mise en œuvre de la première stratégie nationale de cybersécurité (SNC), élaborée en 2012, ont permis à notre pays de réaliser des avancées notables en matière de renforcement de la résilience du cyberspace national et d'amélioration de la sécurité des systèmes d'information nationaux. En 2020 et grâce à ces efforts, notre pays a pu se hisser au 50ème rang de l'index Global Cybersecurity Index (GCI) publié par l'Union Internationale des Télécommunications (UIT).

Le bilan des réalisations au titre de cette stratégie reste en effet largement satisfaisant. Les différentes dimensions de la cybersécurité ont pu être investies, ce qui a permis de doter notre pays d'un cadre juridique et normatif adapté, de diversifier les programmes de renforcement des capacités et de sensibilisation au profit des professionnels, d'identifier les systèmes critiques et d'améliorer notre dispositif de gestion et de réaction aux incidents cybernétiques, notamment par la mise en place du Cert national. Sur le registre de la coopération internationale, plusieurs accords de partenariat avec des organismes étrangers ont été conclus. Ces accords mettent l'accent notamment sur le partage de l'information et l'échange d'expertise.

Dans la continuité de ces efforts et pour rester en phase avec les pratiques à l'international, le Maroc a décidé de mettre à jour sa stratégie nationale de cybersécurité. Le lancement de ce chantier important était l'occasion de prédilection pour dresser une rétrospective des projets achevés, de jeter un regard critique sur notre posture nationale en la matière et d'évaluer notre environnement des risques cyber. Dans le cadre d'une démarche participative, la nouvelle stratégie a fait l'objet durant sa phase préparatoire et aussi au cours de son processus de rédaction de larges consultations auprès des différentes parties prenantes concernées, afin de recueillir leurs avis et prendre en charge leurs besoins.

Conformément aux standards internationaux, la stratégie nationale de cybersécurité, fruit de ce travail, est structurée autour d'une arborescence claire, à même de guider l'action des acteurs et assurer une mise en œuvre efficiente des programmes. Elle repose sur quatre piliers. Chaque pilier est décliné en un ensemble d'objectifs stratégiques et chaque

objectif est traduit en plusieurs initiatives, déployées pour concourir à l'atteinte de l'objectif recherché.

En substance, les quatre piliers de cette stratégie se rapportent à la gouvernance nationale de la cybersécurité, à la sécurité et résilience du cyberspace national, au développement des capacités et la sensibilisation et enfin à la promotion de la coopération régionale et internationale.


Chacun de ces piliers est conçu de manière à répondre à une dimension spécifique de la cybersécurité, allant de l'amélioration du cadre juridique et institutionnel à la prévention des menaces et le renforcement de la résilience des systèmes d'information nationaux, en passant par le développement de compétences et la coopération avec l'étranger.

Le premier pilier de la stratégie met en avant la nécessité de tenir à jour et de renforcer l'arsenal juridique et normatif national régissant la cybersécurité, et ce afin de faire face et suivre l'évolution constante des cybermenaces et leur caractère de plus en plus complexe et sévère. Il prévoit également un volet dédié à l'amélioration de la gouvernance, et ce par l'établissement de mécanismes institutionnels permettant d'optimiser l'action publique et d'asseoir une coordination efficace entre les différents acteurs impliqués dans le domaine de la cybersécurité. C'est le cas notamment des responsables en charge de la protection des infrastructures d'importance vitale, des organes en charge de l'application de la loi et des acteurs du secteur privé.

Sur le plan opérationnel, le deuxième pilier vise à renforcer la sécurité et la défense du cyberspace national face aux différents défis et enjeux inhérents au cyberspace, et ce via la mise en œuvre d'un éventail d'initiatives de nature préventive et réactive. Ces initiatives se rapportent principalement au développement des capacités nationales de détection et de réaction aux attaques cybernétiques et à la promotion de la mise en œuvre de standards et de normes de cybersécurité. Dans le but de soutenir et d'éclairer la prise de décision en matière de cybersécurité, ce pilier accorde une attention particulière au déploiement des mécanismes de recueil de données, de métriques et d'indicateurs.

Comme la valorisation du capital humain demeure au cœur de toute politique ou stratégie publique, le troisième pilier insiste sur l'importance de l'éducation, de la sensibilisation et du développement des compétences. Ce pilier prévoit aussi la création d'un écosystème national de cybersécurité solide et informé, propice au développement de l'innovation et favorable à la croissance d'entreprises spécialisées dans le domaine.

Considérant la nature transfrontalière du cyberspace, la stratégie nationale de cybersécurité ne saurait se suffire des trois précédents piliers sans aborder le volet de la coopération internationale. En établissant des partenariats bilatéraux et multilatéraux avec des institutions internationales et des autorités nationales en charge de la cybersécurité, le Royaume du Maroc réaffirme, à travers cette stratégie, sa volonté de consolider et de garantir la paix et la sécurité du cyberspace mondial. Plusieurs initiatives et actions seront



prévues dans le cadre de ce pilier, qui visent notamment le renforcement du positionnement du Royaume à l'échelle internationale et régionale dans le domaine de la cybersécurité.

Globalement, la stratégie nationale donne la priorité aux aspects juridiques, organisationnels, techniques et de gouvernance, propres à la sécurité et la protection des systèmes d'information. En même temps, elle considère que la coordination entre tous les acteurs, y compris avec les organes en charge de la lutte contre la cybercriminalité est essentielle. Pour cette raison, elle encourage à explorer davantage les possibilités d'entraide, de soutien mutuel et de synergie des ressources.

La stratégie en matière de cybersécurité a pour finalité enfin d'œuvrer pour un cyberspace sûr et résilient, qui est un prérequis indispensable pour soutenir et accompagner la transformation digitale du Royaume. Bien plus qu'un levier de développement socio-économique, la stratégie traduit l'engagement profond du pays à assurer le bien-être et la sécurité des citoyens marocains à l'ère du numérique.

Il convient de préciser que cette stratégie sera appuyée par des plans d'actions détaillés. Le suivi de la mise en œuvre de ces plans d'actions est du ressort de la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI). Conformément à ses attributions, le Comité Stratégique de la Cybersécurité (CSC) procédera à l'évaluation périodique du bilan des réalisations.



INTRODUCTION

Grâce à l'évolution des technologies de l'information et de la communication, le numérique est désormais omniprésent dans tous les domaines de l'activité humaine.

Il a profondément transformé notre vie contemporaine en influençant nos modes de réflexion, de production, de travail, d'apprentissage et de communication. Il a aussi aboli les frontières géographiques en établissant une connectivité mondiale qui a rendu l'information et la connaissance plus accessibles que jamais.

Dans ce contexte, le Royaume du Maroc, sous la conduite éclairée de **Sa Majesté Le Roi**, que Dieu l'Assiste, s'est engagé résolument dans un processus de digitalisation en mettant en œuvre plusieurs programmes et initiatives tels que « Maroc Numeric 2013 » et « Maroc Digital 2020 ». En parallèle, des structures dédiées ont été mises en place afin d'assurer le suivi et réussir la réalisation de ce chantier structurant, considéré comme vital pour notre développement économique et social.

Toutefois, si la digitalisation offre tant d'opportunités, notamment en matière d'inclusion et de développement, elle est accompagnée de risques à gérer, nés des évolutions des usages numériques et des menaces qui lui sont associées. Une digitalisation non maîtrisée constitue, en effet, un terreau fertile à des actes de cyber-malveillance qui pourraient notamment profiter de l'élargissement de la surface d'attaques et viser et perturber l'ordre ou la sécurité publique, l'économie et les services vitaux d'un pays de manière générale.

Conscient de ces enjeux et défis d'ordre sécuritaire et afin d'accompagner la transition numérique, notre pays a choisi de répondre de manière appropriée et globale en procédant à la mise à jour de sa stratégie nationale de cybersécurité. Cette stratégie, fruit de larges consultations avec plusieurs acteurs nationaux, vise à améliorer notre dispositif national de gouvernance et renforcer notre cadre juridique et institutionnel en la matière, tout en mettant l'accent sur l'importance vitale du capital humain dans le domaine de la cybersécurité. La SNC souligne en outre la nécessité d'augmenter les efforts et les investissements pour protéger les systèmes d'information sensibles au niveau national et renforcer leur résilience. Elle dénote également de l'engagement de notre pays au niveau international afin d'instaurer la paix et la sécurité dans le cyberspace.

La cybersécurité est une responsabilité partagée. Pour cela, cette stratégie implique tous les acteurs de l'écosystème national de cybersécurité. Elle fixe les orientations en termes d'objectifs stratégiques et de priorités pour les années à venir. Elle se veut une réponse collective aux enjeux du monde numérique, avec en ligne de mire la mise en place d'un environnement de confiance, propice au développement économique et social de notre pays.

La stratégie nationale de cybersécurité définit les lignes directrices de notre action à l'horizon 2030. Le suivi, la coordination et la supervision de sa mise en œuvre sont du ressort de l'autorité nationale. Elle fera l'objet d'ajustements de manière périodique.



VISION

Pour un cyberspace national fiable, sécurisé et résilient, à même de soutenir la transformation digitale du Royaume, promouvoir la prospérité économique et assurer le bien-être des citoyens





LA CYBERSECURITE AU MAROC

Paysage des menaces et cyber risques

Le Royaume du Maroc, dans une démarche proactive de protection de son cyberspace, a réalisé une étude visant à apprécier les risques cybernétiques au niveau national. Cette étude avait pour vocation d'établir un inventaire détaillé des menaces pesant sur le cyberspace national et d'orienter ainsi les efforts en matière de cybersécurité.

Les résultats de cette étude ont révélé une concordance significative entre les défis cybernétiques de notre pays et ceux rencontrés à l'échelle mondiale. Cette similitude met en évidence l'universalité de la menace cybernétique et souligne l'importance d'une prise de conscience mondiale face à ce défi.

Parmi les nombreuses menaces cybernétiques identifiées, plusieurs se distinguent par leur fréquence d'occurrence et leur potentiel de destruction :

- ▶ Les rançongiciels, capables de paralyser les activités d'une entreprise ou d'un service public, avec des impacts importants sur le plan économique et aussi en termes de réputation.
- ▶ Les attaques DDoS, qui peuvent rendre inaccessibles les services en ligne, entraînant d'importants préjudices.
- ▶ L'ingénierie sociale, qui consiste à manipuler les utilisateurs pour les amener à divulguer des informations confidentielles ou à effectuer des actions mettant en danger leur propre sécurité ou celle des systèmes d'information de leurs organisations.

Cette étude a mis en lumière, en outre, le risque lié à la sécurité de la chaîne d'approvisionnement, ainsi que les défis en matière de cybersécurité posés par certaines nouvelles tendances comme l'intelligence artificielle, l'Internet des Objets et le Big Data. L'évolution rapide de ces technologies requiert une veille constante et une adaptation des stratégies mises en place pour faire face aux menaces émergentes.

Acquis de la Stratégie Nationale en matière de cybersécurité 2012

Depuis l'adoption de la première Stratégie Nationale de Cybersécurité (SNC) en 2012, le Royaume du Maroc a accompli des progrès notables en matière de renforcement de la sécurité et de la résilience de son cyberspace.

Sur le plan réglementaire, la stratégie a conduit à l'élaboration d'un cadre juridique et normatif dédié à la cybersécurité. Il s'agit en particulier de loi sur la cybersécurité et son décret d'application et de la Directive Nationale de la Sécurité des Systèmes d'Information.

En matière de renforcement des capacités, notre pays a mis en œuvre des programmes diversifiés de formation et de sensibilisation visant à élever le niveau de compétence des professionnels exerçant dans le secteur de la cybersécurité. Parmi les actions réussies dans ce cadre figure la création d'un cursus de formation en cybersécurité sous forme de Master spécialisé.

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 infrastructures d'importance vitale (IIV) et d'identifier les systèmes d'information considérés sensibles pour l'Etat. En outre, les missions d'audit menées annuellement par la DGSSI ont favorisé le développement de la culture du contrôle et de l'évaluation.

En ce qui concerne la gestion des incidents, la SNC a aussi contribué au renforcement des capacités des organismes publics et des IIV à gérer les incidents de cybersécurité en les incitant à mettre en place des centres opérationnels de sécurité (SOC). Ces centres ont pour mission de surveiller, de détecter, d'analyser et de réagir auxdits incidents, et ce sous l'égide du centre de veille, détection et réponse aux attaques informatiques (maCERT) relevant de la DGSSI.

En termes de mise à niveau de l'écosystème national de cybersécurité, des régimes de qualification ont été mis en place. Ces régimes ont pour objectif d'encadrer l'activité des prestataires de cybersécurité et des prestataires d'audit de la sécurité des systèmes d'information, souhaitant fournir leurs services aux IIV disposant de SIS, et ce afin de disposer de garanties réelles sur la qualité des services fournis.

Sur le front de la coopération internationale, ladite stratégie a favorisé l'établissement et la signature de plusieurs accords de partenariat avec des organismes étrangers. Ces accords mettent l'accent notamment sur l'échange de l'information, de l'expertise et des bonnes pratiques en matière de cybersécurité.

Cadre institutionnel

Organes en charge de la sécurité des systèmes d'information

En matière de gouvernance, la sécurité des systèmes d'information et la protection du cyberspace national relèvent des attributions des acteurs institutionnels suivants :

► 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 du bilan d'activité de la DGSSI et des travaux du comité national de gestion des crises et événements cybernétiques majeurs. Par ailleurs, il arrête le périmètre des audits de la sécurité des systèmes d'information effectués par la DGSSI.

Il est chargé également de donner son avis sur les projets de lois et de textes 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 événements cybernétiques majeurs est chargé d'assurer une intervention coordonnée en matière de prévention et de gestion de crise suite à des incidents de cybersécurité. Il peut décider des mesures que les responsables des entités et des infrastructures d'importance vitale doivent mettre en œuvre. Il adresse aussi des recommandations et des conseils aux opérateurs du secteur privé et aux particuliers.

► **La Direction Générale de la Sécurité des Systèmes d'Information**

La DGSSI est l'autorité nationale de la cybersécurité chargée de coordonner les travaux relatifs à l'élaboration et à la mise en œuvre de 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 et de définir des mesures de protection des systèmes d'information et veiller à leur application. Elle est responsable, par ailleurs, de la qualification des prestataires d'audit des systèmes d'information et ceux des services de cybersécurité.

La DGSSI a pour mission également 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.

Organes en charge de la lutte contre la cybercriminalité

En fonction de leurs attributions respectives, les organes suivants exercent des attributions dans le domaine de la lutte contre la cybercriminalité :

- Le Ministère de la Justice
- Le Conseil Supérieur du Pouvoir Judiciaire
- La Présidence du Ministère Public (PMP)
- La Direction Générale de la Sûreté Nationale (DGSN)
- La Gendarmerie Royale (GR)

Sur le plan organisationnel, ces acteurs disposent d'unités et de structures dédiés à la lutte contre la cybercriminalité.

La Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel

La Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP) est chargée de vérifier que les traitements des données personnelles sont licites, légaux et qu'ils ne portent pas atteinte à la vie privée, aux libertés et droits fondamentaux de l'Homme.

Cadre juridique et normatif national propre à la cybersécurité

Le paysage juridique et normatif marocain en matière de cybersécurité a connu des évolutions notables au cours de la dernière décennie. L'adoption progressive de plusieurs textes législatifs et réglementaires illustre une prise de conscience et un engagement continu envers la protection de notre espace numérique.

A cet égard, la première brique a été posée par la DGSSI en 2014 suite à l'élaboration de la Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI). Cette directive a pour objectif de renforcer 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, en précisant les mesures de sécurité organisationnelles et techniques minimales à appliquer.

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 vu le jour. Ce décret définit les règles de sécurité applicables aux infrastructures d'importance vitale disposant des systèmes d'information sensibles, et ce dans le but de renforcer leur résilience et garantir leur continuité de fonctionnement.

En 2018, 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 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.

En 2020, le corpus juridique a été revisité par la promulgation loi n° 05-20 relative à la cybersécurité. Cette loi préconise les moyens de protection et de résilience visant à développer la confiance numérique, en fixant les règles et les dispositions de sécurité applicables à l'ensemble des acteurs de l'écosystème numérique, dont notamment les entités, les infrastructures d'importance vitales et les opérateurs. La loi permet aussi d'arrêter le cadre et les structures de gouvernance de la cybersécurité, de renforcer le cadre de collaboration et d'échange avec les partenaires nationaux et étrangers.

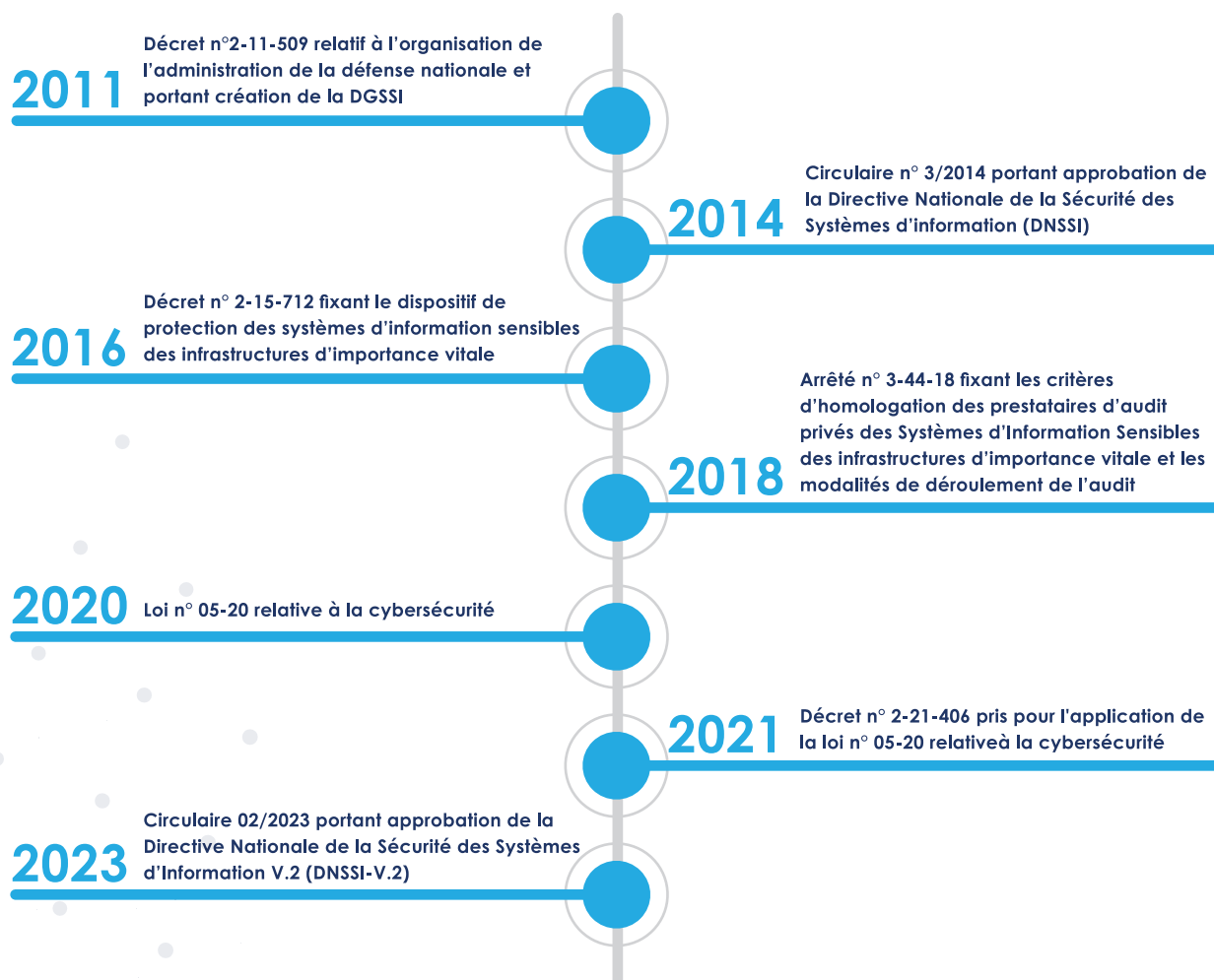
Pour permettre l'entrée en vigueur de la loi, l'année 2021 a été marquée par la publication du décret d'application. Ce texte réglementaire fixe la composition et les modalités de fonctionnement des organes de gouvernance de la cybersécurité, prévus par la loi n° 05-20, à savoir l'autorité nationale de la cybersécurité, le comité stratégique de la cybersécurité et le comité de gestion des crises et événements cybernétiques majeurs. Ledit



décret détaille les dispositions propres aux entités et aux IIV 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.

Dans la continuité de ces efforts, la DGSSI a procédé en 2023 à la mise à jour de la Directive Nationale de la Sécurité des Systèmes d'Information de 2014. Cette mise à jour intervient pour prendre en considération les changements apportés au cadre juridique et normatif et aussi les bonnes pratiques applicables dans le domaine de la sécurité des systèmes d'information.

Il convient de souligner enfin que la DGSSI, conformément à ses attributions, a élaboré et publié plusieurs directives, 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.





PILIERS STRATEGIQUES



PILIER 1



GOVERNANCE NATIONALE DE LA CYBERSÉCURITÉ : CADRE INSTITUTIONNEL ET JURIDIQUE

L'évolution continue de l'environnement des technologies de l'information et de la communication s'accompagne forcément par une mutation de l'environnement des risques et menaces. Une telle situation appelle des efforts soutenus pour la revue et l'adaptation du corpus juridique national applicable à la cybersécurité, de manière à prendre en considération les nouveaux enjeux et aussi anticiper les défis futurs.

Sur le plan institutionnel, la mise en place d'un cadre de coordination et de coopération entre les différents acteurs revêt une importance capitale. La mise en commun des compétences et des ressources de manière générale est de nature à optimiser l'action publique et apporter des réponses appropriées aux défis de cybersécurité.

Améliorer les mécanismes de coordination nationale

Initiative 1.2.1

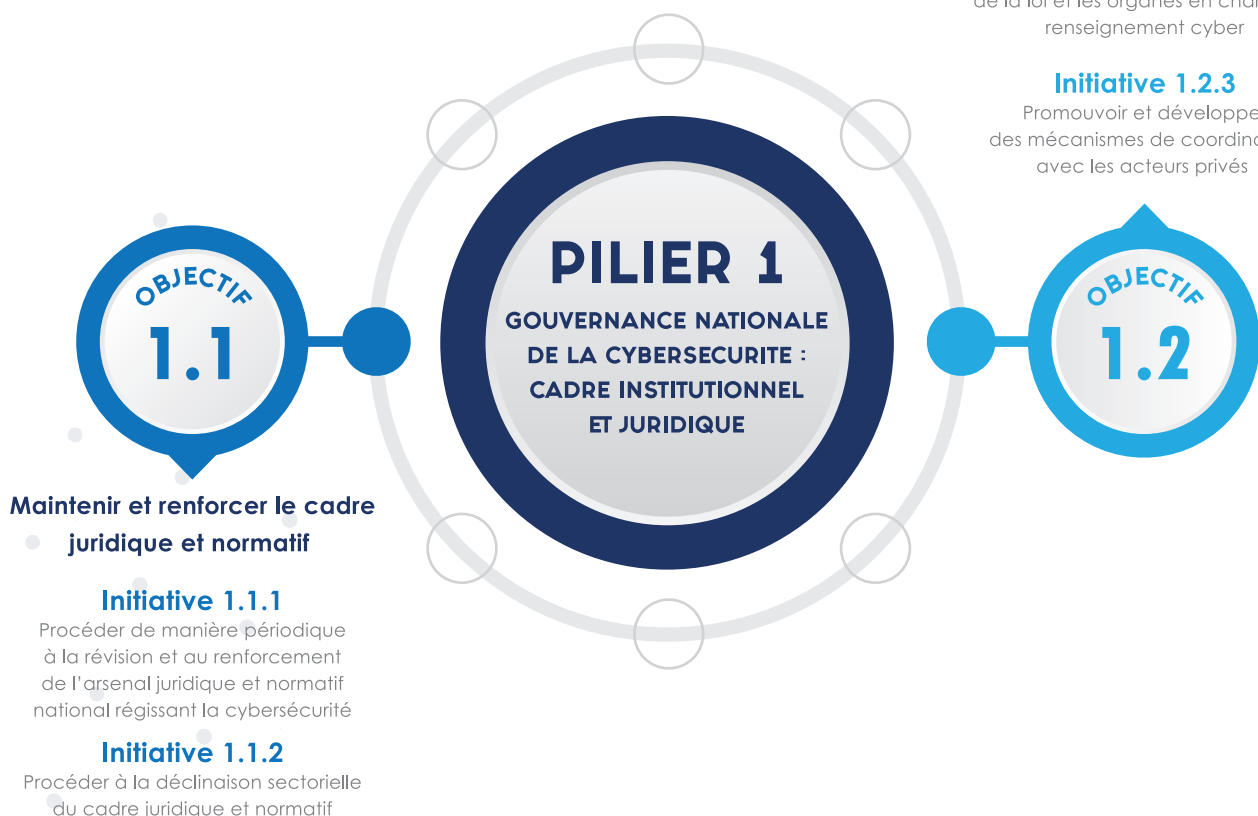
Améliorer la coordination et le partage d'informations entre les intervenants en matière de protection des IIV

Initiative 1.2.2

Améliorer la coordination entre les organes en charge de l'application de la loi et les organes en charge du renseignement cyber

Initiative 1.2.3

Promouvoir et développer des mécanismes de coordination avec les acteurs privés



Objectif 1.1 : Maintenir et renforcer le cadre juridique et normatif

► Procéder de manière périodique à la révision et au renforcement de l'arsenal juridique et normatif national régissant la cybersécurité.

L'objectif recherché à travers cette initiative est de procéder de manière régulière à la revue des textes législatifs et réglementaires et aussi du corpus normatif applicable à la cybersécurité, et ce afin de s'assurer que ceux-ci sont à jour et sont conformes aux pratiques internationales en vigueur. Ce travail doit être mené, en toute logique, en concertation avec les administrations et les parties prenantes concernées.

Pour atteindre l'objectif assigné, il est primordial d'exercer à la fois une veille sur les technologies numériques utilisées et aussi sur le paysage de la cybersécurité. Cette veille doit englober entre autres l'étude des tendances, des techniques d'attaque, des innovations technologiques et des évolutions juridiques et normatives au niveau international.

► Procéder à la déclinaison sectorielle du cadre juridique et normatif

La déclinaison sectorielle du cadre juridique et normatif consiste en l'extension de ce cadre et son adaptation aux spécificités propres aux différents secteurs d'activité.

Cette démarche va permettre d'élargir le périmètre couvert et aussi d'assurer une protection appropriée et proportionnelle aux risques auxquels chaque secteur devrait être confronté.

Ce travail, qui doit se baser sur des évaluations préalables des enjeux et des risques spécifiques à chaque secteur d'activité, sera conduit de manière progressive et selon une approche mettant à contribution, d'une part, la DGSSI en sa qualité d'autorité nationale en charge de la cybersécurité et, d'autre part, les régulateurs et les institutions qui sont en charge de la supervision des risques et de la coordination sectorielle. Cette synergie permettra de concevoir des cadres répondant aux particularités spécifiques à chaque secteur et facilitera par la suite l'implémentation et le suivi du respect des règles édictées.

Il est précisé enfin que la priorité sera accordée dans le cadre de cette initiative aux secteurs d'importance vitale.

Objectif 1.2 : Améliorer les mécanismes de coordination nationale

► Améliorer la coordination et le partage d'informations entre les intervenants en matière de protection des II

L'importance des infrastructures d'importance vitale ainsi que leur interdépendance requièrent une coordination étroite entre les parties prenantes concernées par la protection desdites infrastructures. La mise en place d'un cadre de coopération vise à conjuguer les initiatives, les moyens et l'expertise pour assurer une intervention efficace face aux cybermenaces pesant sur les systèmes d'information sensibles.

A cet égard, des cadres de partage d'informations seront déployés, rassemblant les différents intervenants concernés, et ce sous l'égide de la DGSSI. Ces espaces d'échange



auront l'avantage de faciliter la circulation d'informations utiles et la communication des données concernant notamment les menaces, les incidents et les bonnes pratiques en matière de cybersécurité, ce qui permet, par conséquent, de renforcer in fine la résilience des IIIV et leur capacité de reprise.

Dans le cadre de cette initiative, il est également question d'établir des conventions ou des mémorandums d'entente entre l'autorité nationale en charge de la cybersécurité et les coordonnateurs sectoriels afin de mettre en place les cadres d'échange suscités et aussi pour clarifier et définir les rôles et responsabilités de chaque partie en matière de protection des IIIV et leurs systèmes d'information sensibles.

► **Améliorer la coordination entre les organes en charge de l'application de la loi et les organes en charge du renseignement cyber**

La coordination entre les organes chargés de l'application de la loi, les organes en charge du renseignement cyber et l'autorité en charge de la cybersécurité s'avère primordiale pour faire face et monter en efficacité contre les assauts cybernétiques. Il est ainsi nécessaire d'instaurer des canaux de communication garantissant la fluidité des échanges, tout en préservant la confidentialité et l'intégrité des informations partagées.

La mise en place d'un tel cadre de coordination permet de renforcer la capacité du pays à détecter et à analyser les menaces de manière proactive, et ce en s'appuyant sur les renseignements et les données collectées par chaque organe.

En matière d'investigations liées à la cybercriminalité, la collaboration entre ces acteurs constitue un moyen incontournable pour approfondir les enquêtes et traduire en justice les auteurs d'actes malveillants. À cette fin, des procédures opérationnelles seront établies et auront pour objectif de déterminer les apports potentiels des acteurs, et ce dans le respect de leurs mandats et missions respectifs.

Il est envisageable également de mutualiser les efforts de ces organes dans le domaine de la formation, et ce afin de renforcer leur capacité globale à protéger le cyberspace national face aux menaces cyber.

► **Promouvoir et développer des mécanismes de coordination avec les acteurs privés**

Un nombre important de systèmes d'information nationaux sont confiés et gérés par des acteurs privés. Cette initiative vise à mutualiser les efforts, les expertises et les ressources des secteurs public et privé pour aborder les problématiques de sécurité numérique de manière globale et efficace.

Afin de concrétiser cet objectif, notre pays compte, en étroite collaboration avec les principaux acteurs privés œuvrant dans le domaine de la cybersécurité, de mettre en place des mécanismes de coordination et des plateformes d'échange d'information par rapport aux menaces et aux vulnérabilités identifiées.

En outre, il est envisageable d'établir des partenariats, notamment dans les domaines de développement des capacités, de la formation, de la sensibilisation, de l'innovation et du développement de solutions et de services de cybersécurité.

PILIER 2



SÉCURITÉ ET RÉSILIENCE DU CYBERESPACE NATIONAL

Le Maroc compte renforcer la sécurité et la résilience de son cyberspace national face aux défis croissants qui émanent du cyberspace. L'action publique poursuit comme objectifs de préserver les intérêts vitaux de la nation, garantir la continuité des services essentiels et protéger les données et les systèmes d'information sensibles.

Dans cette perspective, notre pays envisage de déployer, dans le cadre de ce pilier, un ensemble de mesures et d'initiatives visant à anticiper et à prévenir les menaces et les vulnérabilités qui pèsent sur son cyberspace. Cette approche globale se traduira notamment par le développement de capacités nationales de détection et de réaction aux attaques informatiques et par la promotion de la mise en œuvre de standards et de normes de cybersécurité.

Appuyer la prise de décision et soutenir les politiques fondées sur les données (data-Driven)

Initiative 2.1.1

Disposer d'un état des lieux du paysage national de cybersécurité

Initiative 2.1.2

Mettre en place des mécanismes de recueil de données, de métriques et d'indicateurs sur les capacités nationales en matière de cybersécurité

OBJECTIF

2.1

Renforcer la protection des systèmes d'information des infrastructures vitales

Initiative 2.4.1

Tenir à jour une cartographie des IIV et de leurs SIS et clarifier les dépendances intersectorielles

Initiative 2.4.2

Renforcer les activités d'audit et de contrôle pour la vérification de la conformité des IIV

Initiative 2.4.3

Renforcer la résilience des opérateurs télécom et opérateurs de services numériques

OBJECTIF

2.2

Promouvoir la mise en œuvre de standards et de normes de cybersécurité

Initiative 2.2.1

Renforcer l'offre existante par la mise en place de nouveaux schémas de qualification et de labellisation des produits et des prestations de cybersécurité

Initiative 2.2.2

Mettre en place des schémas nationaux de certification en matière de cybersécurité pour les organismes publics et privés

PILIER 2

SÉCURITÉ ET RÉSILIENCE
DU CYBERESPACE
NATIONAL

OBJECTIF

2.4

Renforcer les capacités nationales de prévention, de gestion et de réaction aux incidents et crises cybernétiques

Initiative 2.3.1

Renforcer la préparation nationale et la réactivité pour faire face aux crises cybernétiques

Initiative 2.3.2

Développer des capacités sectorielles en matière de gestion des incidents cybernétiques

OBJECTIF

2.3

Objectif 2.1 : Appuyer la prise de décision et soutenir les politiques fondées sur les données

► Disposer d'un état des lieux du paysage national de cybersécurité

Après les premières études d'évaluation de la maturité et des risques cybernétiques, notre pays envisage pour une meilleure maîtrise de sa posture nationale, de poursuivre les efforts pour analyser et diagnostiquer son paysage de cybersécurité en adoptant une approche méthodique basée sur des revues périodiques des forces et faiblesses du pays dans ce domaine.

Cette initiative a pour objectif de mettre en place un tableau de bord des suivis et permettre aux décideurs de disposer d'une vision globale et éclairée des enjeux de cybersécurité auxquels le pays doit faire face, de mesurer les progrès accomplis au fil des années et d'ajuster, en conséquence, les politiques et stratégies mises en œuvre.

► Mettre en place des mécanismes de recueil de données, de métriques et d'indicateurs sur les capacités nationales en matière de cybersécurité

La mise en place de mécanismes de recueil de données, de métriques et d'indicateurs relatifs aux capacités nationales en matière de cybersécurité se présente comme une démarche essentielle pour affronter et anticiper les enjeux et les défis inhérents au cyberspace.

A cet égard, il est envisageable, dans le cadre de cette initiative, de mettre en place une structure qui sera chargée de la collecte, de l'analyse et de la diffusion d'informations pertinentes sur les cybermenaces et les incidents de cybersécurité. Elle permettra également d'évaluer l'efficacité des actions entreprises pour renforcer la résilience du pays face aux cyberattaques.

Ainsi, cette structure joue un rôle déterminant dans la consolidation des données recueillies, leur transformation en indicateurs et métriques pertinents et la mise à disposition des décideurs des informations nécessaires pour ajuster et affiner les politiques de cybersécurité. Ce processus permet aussi une meilleure compréhension des enjeux et des tendances du paysage numérique et facilite ainsi l'adoption de mesures proactives pour contrer les cybermenaces et protéger notre cyberspace national.

Objectif 2.2 : Promouvoir la mise en œuvre de standards et de normes de cybersécurité

► Renforcer l'offre existante par la mise en place de nouveaux schémas de qualification et de labellisation des produits et des prestations de cybersécurité

L'introduction de nouveaux schémas de qualification et de labellisation des produits et des prestations de cybersécurité est une démarche qui a pour objectif de cibler de nouveaux services et d'élargir la gamme des solutions de cybersécurité qui jouissent d'un niveau de confiance élevé. Le recours à ces produits et services va permettre de renforcer davantage la sécurité des systèmes d'information sensibles.

En outre, l'adoption de tels schémas de qualification et de labellisation contribuera au renforcement de la résilience du cyberspace national face aux cybermenaces en instaurant une culture de cybersécurité où l'excellence et la compétence sont valorisées.

Il convient de souligner que ce travail s'inscrit dans la continuité des actions déjà accomplies, à savoir le régime de qualification des prestataires d'audit de la sécurité des systèmes d'information et celui des prestataires de cybersécurité. La mise en place de tels régimes vise à apporter les garanties nécessaires quant au niveau de service et aux performances de ces produits et prestations, et ce dans le but de rassurer les équipes informatiques et les donneurs d'ordre de manière générale.

► **Mettre en place des schémas nationaux de certification en matière de cybersécurité pour les organismes publics et privés**

Cette initiative a pour but de reconnaître et de récompenser les efforts des organismes publics et privés désireux d'obtenir lesdites certifications et aussi de valoriser leur action en matière de protection de leurs systèmes d'information, et ce en se basant sur des référentiels d'exigences de sécurité.

L'obtention de telles certifications permettra également de renforcer la crédibilité et la notoriété de ces organismes sur les marchés nationaux et internationaux en rassurant leurs partenaires quant à la fiabilité et la sécurité de leurs infrastructures et services numériques et à l'importance qui leur est accordée.

Objectif 2.3 : Renforcer les capacités nationales de prévention, de gestion et de réaction aux incidents et crises cybernétiques

► **Renforcer la préparation nationale et la réactivité pour faire face aux crises cybernétiques**

La gestion des crises et des événements cybernétiques revêt une importance cruciale pour réduire au minimum les dommages potentiels et rétablir la sécurité et la stabilité des systèmes d'information. À cet égard, le Maroc a élaboré un dispositif de gestion de crise visant à encadrer et à préciser les missions ainsi que les responsabilités des membres du comité de gestion des crises.

Pour améliorer constamment les capacités de ce comité, il est essentiel de mettre à jour régulièrement les plans et les procédures afin de faire face à l'évolution des menaces et des technologies. Il convient également d'organiser régulièrement des exercices de gestion de crise et de former et sensibiliser le personnel à la gestion des crises.

► **Développer des capacités sectorielles en matière de gestion des incidents cybernétiques**

Afin de développer des capacités sectorielles en matière de gestion des incidents cybernétiques, notre pays entend encourager la mise en place de CERTs (Computer Emergency Response Team) sectoriels au niveau des régulateurs et coordonnateurs des secteurs d'importance vitale.

Ces CERTs sectoriels joueront un rôle clé dans la détection, l'analyse, la prévention et la réponse aux incidents cybernétiques touchant leurs secteurs respectifs. Ils permettront également de faciliter la communication et la coordination avec les autorités nationales compétentes, y compris le maCERT national.

Il est également envisageable de mettre en œuvre, dans le cadre de cette initiative, des programmes de renforcement de capacités ciblant des infrastructures d'importance vitale. Ces programmes visent à renforcer les compétences techniques de leurs ressources humaines en termes de gestion des incidents et d'encourager la création, en leur sein, de centres opérationnels de sécurité (SOC).



Objectif 2.4 : Renforcer la protection des systèmes d'information des infrastructures vitales

► Tenir à jour une cartographie des IIV et de leurs SIS et clarifier les dépendances intersectorielles

Les infrastructures et les services essentiels qui soutiennent notre sécurité, notre économie et notre bien-être sont de plus en plus tributaires des technologies de l'information et de l'usage du numérique. Cette dépendance croissante, bien que source de progrès, rend également ces infrastructures vulnérables aux cyberattaques.

Face à cette réalité, la DGSSI a entrepris, dans un premier temps, un travail de recensement des IIV et des SIS, en impliquant les acteurs concernés, tant publics que privés. Cette démarche a permis d'identifier et de cartographier les infrastructures et les services indispensables au fonctionnement du pays ainsi que les systèmes d'information qui les supportent.

S'inscrivant dans la même logique, il est prévu de procéder de manière régulière à la mise à jour de la liste des IIV et leurs SIS pour prendre en compte les changements qui pourraient affecter les rôles des IIV recensées et le degré de criticité de leurs missions et de leurs systèmes.

Dans le même sillage, il sera procédé à la cartographie des dépendances intersectorielles, et ce afin de repérer les liens et les interactions éventuelles entre les systèmes d'information sensibles et de cerner les répercussions possibles en cas d'attaque ou d'incident de cybersécurité sur l'ensemble du cyberspace national. En effet, l'examen approfondi de ces interdépendances permet d'identifier les points potentiels de vulnérabilité et d'anticiper les effets post-incident.

► **Renforcer les activités d'audit et de contrôle pour la vérification de la conformité des infrastructures d'importance vitale**

Conscient de l'importance cruciale des infrastructures d'importance vitale pour la sécurité nationale, l'économie et la société, notre pays prévoit de multiplier les opérations d'audit et de contrôle de conformité.

Pour ce faire, il est prévu de mobiliser l'expertise et les compétences de la DGSSI et des prestataires d'audit privés pour assurer un niveau élevé d'exigence et de professionnalisme lors de l'évaluation de ces infrastructures critiques. Les audits et les contrôles prévus porteront notamment sur l'identification des vulnérabilités potentielles, sur l'évaluation des risques associés et de manière générale, sur la vérification de la conformité aux normes et réglementations en vigueur.

À l'issue de ces opérations d'audit, des plans d'actions seront élaborés pour remédier aux faiblesses identifiées et pour mettre en place des mesures de protection adaptées. Ces plans d'actions constitueront une feuille de route pour l'autorité nationale et pour les organismes responsables des IIV, incluant des recommandations et des actions correctives nécessaires.

► **Renforcer la résilience des opérateurs télécom et opérateurs de services numériques**

Avec l'avancée de la digitalisation, les services d'infrastructures offerts par les opérateurs de télécommunication et les opérateurs de services numériques (comme les hébergeurs, les fournisseurs cloud, etc.) gagnent en importance et en criticité.

Bien qu'assujettis à des exigences particulières au même titre que les infrastructures d'importance vitale des autres secteurs, ces opérateurs doivent faire l'objet d'une attention particulière compte tenu de l'impact généralisé et étendu que peut avoir un incident sur leurs plateformes.

Cette initiative vise à renforcer la résilience de ces opérateurs, considérés comme supports indispensables à tous les secteurs stratégiques, et ce moyennant une approche multidimensionnelle qui allie des actions aussi bien d'ordre réglementaire et normatif que technique afin d'assurer une haute disponibilité et une capacité étendue de reprise d'activité en cas d'incident.

PILIER 3



DÉVELOPPEMENT DES CAPACITÉS ET SENSIBILISATION

Dans la perspective de construire un avenir digital sécurisé et résilient, le Royaume du Maroc s'engage à intensifier son approche axée sur le développement des capacités et la sensibilisation en matière de cybersécurité. Cette démarche vise à augmenter le degré de connaissance, d'expertise et de sensibilisation aux questions de cybersécurité auprès de l'ensemble de la société marocaine.

Dans ce sens, un éventail d'initiatives stratégiques sera déployé. Ces initiatives se rapportent notamment à la sensibilisation des citoyens aux risques et menaces du cyberspace, au lancement de campagnes de sensibilisation dédiées au secteur privé et à l'instauration de modules d'éveil à la cybersécurité au sein des programmes scolaires.

Par ailleurs, un intérêt particulier sera accordé à l'enrichissement et l'augmentation des cursus de formation en matière de cybersécurité dans les universités et centres de formation professionnelle. En parallèle, le recours à la certification professionnelle sera vivement encouragé, et ce dans le but de constituer un vivier d'experts certifiés en cybersécurité aptes à relever les défis de ce domaine complexe.

Dans le même cadre, notre pays ambitionne de créer un environnement favorable à l'émergence et au développement des innovations en matière de cybersécurité. Cette dynamique vise à stimuler l'écosystème national et favoriser l'essor d'entreprises spécialisées en la matière.



Développer une culture de cybersécurité au sein de la société

Initiative 3.1.1

Sensibiliser les citoyens sur les menaces et les risques de sécurité inhérents au cyberspace

Initiative 3.1.2

Mettre en place des campagnes de sensibilisation au profit des secteurs public et privé

Initiative 3.1.3

Introduire des modules de sensibilisation à la cybersécurité au niveau scolaire



Soutenir le développement de l'écosystème national de cybersécurité et encourager l'innovation

Initiative 3.3.1

Encourager le développement de l'écosystème de cybersécurité à l'échelle nationale

Initiative 3.3.2

Soutenir la recherche et développement au sein des universités et des centres de formation



Renforcer les capacités des ressources humaines en matière de cybersécurité

Initiative 3.2.1

Mettre à niveau et augmenter les cursus de formation en cybersécurité dans les universités et les centres de formation professionnelle

Initiative 3.2.2

Encourager la certification professionnelle afin de constituer un vivier d'experts certifiés en cybersécurité

Initiative 3.2.3

Améliorer l'offre de la formation continue pluridisciplinaire au profit des gestionnaires de la cybersécurité

Initiative 3.2.4

Adapter l'offre de formations en cybersécurité aux besoins métiers

Objectif 3.1 : Développer une culture de cybersécurité au sein de la société

► Sensibiliser les citoyens sur les menaces et les risques de sécurité inhérents au cyberspace

Le cyberspace est un domaine partagé par tous les acteurs de la société, qu'ils soient publics ou privés, individuels ou collectifs. Il est donc nécessaire que chacun prenne conscience de ses obligations dans cet espace, ainsi que des conséquences de ses actions.

Les citoyens sont souvent les premières victimes ou les premiers vecteurs des cyberattaques. Par manque de connaissance ou de vigilance, ils peuvent être cibles d'attaques de phishing pour le vol de leurs données personnelles, être manipulés par des campagnes d'influence ou subir des atteintes à leurs vies privées.

Une sensibilisation à large échelle des citoyens à la cybersécurité permet de renforcer les comportements responsables et inciter à l'adoption des bonnes pratiques notamment en ligne, afin de réduire les vulnérabilités et de se protéger contre les menaces potentielles.

Former et éduquer les citoyens aux enjeux de la sécurité du numérique est tout aussi stratégique. En effet, un citoyen averti, capable de respecter les règles élémentaires de cyber-hygiène, serait en mesure de se protéger aussi bien sur le plan personnel que professionnel, ce qui ne ferait qu'augmenter la résilience collective de notre société face aux cyber-attaques.

► Mettre en place des campagnes de sensibilisation au profit des secteurs public et privé

La cybersécurité est un facteur clé de succès pour les entreprises, qui doivent prendre conscience des risques et se doter des moyens nécessaires pour se défendre contre les cyberattaques. La sensibilisation du secteur privé à la cybersécurité est indispensable pour renforcer la résilience et par ricochet la compétitivité des entreprises nationales.

Au-delà des grandes entreprises qui opèrent dans des secteurs vitaux de la nation et qui sont naturellement la cible privilégiée des attaquants, les PME et TPE sont désormais de plus en plus exposées aux cyberattaques et aux cyber escroqueries, car elles sont plus vulnérables et moins outillées.

Une cyberattaque peut avoir des conséquences graves sur la continuité d'activité, la réputation et la compétitivité d'une entreprise indépendamment de sa taille. A ce titre, il est essentiel de sensibiliser tous les acteurs du secteur privé aux risques de cybersécurité et de les aider à se protéger efficacement, notamment dans le cadre de campagnes ciblées ayant pour objectifs de :

- Démontrer l'importance de la mise en conformité aux référentiels nationaux en matière de cybersécurité ;
- Promouvoir l'adoption d'une démarche de gestion des risques, qui permet d'identifier les actifs sensibles, les menaces potentielles et les mesures de protection adaptées ;
- Inciter à la formation et la sensibilisation des collaborateurs aux impératifs de sécurité numérique ;
- Encourager le recours à l'expertise qualifiée pour réaliser des audits de sécurité ou des prestations de conseil.

Parallèlement, il est envisageable de poursuivre les efforts de sensibilisation, initiés ces dernières années, au profit du secteur public, et ce afin de s'assurer que toutes les sphères de l'administration soient pleinement conscientes et préparées face aux enjeux de cybersécurité

► Introduire des modules de sensibilisation à la cybersécurité au niveau scolaire

La cybersécurité est un domaine de plus en plus important et stratégique dans le monde numérique actuel. Elle concerne la protection des données, des systèmes, des réseaux et des services contre les attaques malveillantes qui peuvent avoir des impacts négatifs sur la vie privée, l'économie, ou la sécurité. Pour cela, il est important de développer la culture de la sécurité numérique dès le plus jeune âge, et ce en introduisant des modules de sensibilisation au niveau scolaire.

Les élèves sont des utilisateurs fréquents et parfois imprudents des technologies numériques. Ils sont exposés à des risques tels que le cyberharcèlement, le vol d'identité, l'usurpation de comptes, le piratage et la désinformation.

Leur sensibilisation à la cybersécurité va leur permettre d'acquérir des connaissances et d'adopter des comportements responsables et éthiques sur Internet. Elle les aide à se protéger contre les cybermenaces, à respecter les droits et les devoirs liés à l'utilisation du numérique et à développer un esprit critique face aux informations en ligne.

La sensibilisation à la cybersécurité peut aussi être considérée comme une première immersion dans les domaines du numérique, qui sont porteurs d'emplois et d'innovation. Elle permet aux élèves de découvrir les enjeux, les acteurs, les outils et les bonnes pratiques de la cybersécurité, et de s'initier aux notions de base de la programmation et de l'analyse de données ou encore de la cryptographie.

Il importe de préciser, enfin, que les modules de sensibilisation à la cybersécurité au niveau scolaire doivent impérativement être adaptés sur le plan pédagogique à l'âge et au niveau des élèves.

Objectif 3.2 : Renforcer les capacités des ressources humaines en matière de cybersécurité

► Mettre à niveau et augmenter les cursus de formation en cybersécurité dans les universités et les centres de formation professionnelle

Cette initiative vise à former une nouvelle génération de spécialistes de la cybersécurité capables de défendre le cyberspace national et de protéger les informations et les infrastructures d'importance vitale du pays. Les spécialistes de la cybersécurité constituent en effet une ligne de défense contre les cybermenaces, qui ne cessent d'évoluer tant sur le plan de l'intensité que sur le plan de la complexité technique.

Face à cette prolifération des cybermenaces, il existe actuellement une pénurie mondiale de professionnels qualifiés. Pour combler ce besoin, il est nécessaire de former au niveau national de plus en plus d'experts en cybersécurité et de maintenir à jour leurs connaissances techniques. Il convient donc d'augmenter et de diversifier les cursus de formation en cybersécurité dans les universités et les centres de formation professionnelle et aussi de revisiter les curricula pour les mettre à niveau.



Cette initiative ne peut réussir sans une collaboration active entre le secteur de l'enseignement et les secteurs public et privé pour former des professionnels capables de relever les défis complexes de sécurité auxquels ces derniers sont confrontés.

Elle devra aussi être accompagnée d'une action de promotion de ces programmes de formation pour attirer des étudiants talentueux et passionnés ainsi que d'une sensibilisation des entreprises et des employeurs de manière générale aux avantages de recruter des ressources diplômées.

► **Encourager la certification professionnelle afin de constituer un vivier d'experts certifiés en cybersécurité**

Encourager la certification professionnelle en cybersécurité est un moyen efficace de constituer un vivier d'experts qualifiés et certifiés dans ce domaine. Les certifications offrent une validation formelle des compétences et des connaissances des professionnels, ce qui peut renforcer leur crédibilité et aussi leur employabilité.

Les certifications en cybersécurité attestent que les professionnels possèdent les compétences et les connaissances nécessaires pour relever les défis de sécurité informatique. Elles sont généralement basées sur des normes reconnues par l'industrie, ce qui garantit que les détenteurs de certifications sont alignés sur les meilleures pratiques en la matière.

Les certifications permettent aussi de simplifier les processus d'embauche ou de sélection de candidats pour occuper un poste ou rendre une prestation. Les employeurs peuvent donc intégrer ces certifications parmi les critères de sélection afin d'identifier les candidats qualifiés.

► **Améliorer l'offre de formation continue pluridisciplinaire au profit des gestionnaires de la cybersécurité**

La formation continue est une composante essentielle de toute stratégie de renforcement des capacités. En effet, les attaques et les techniques cybercriminelles évoluent rapidement. Les professionnels de la cybersécurité ont besoin d'une formation continue pour rester à jour avec les dernières tendances et méthodes d'attaque.

Les avancées technologiques aussi, telles que l'Internet des objets (IdO), l'intelligence artificielle (IA) et la 5G, présentent de nouveaux défis en matière de sécurité. Les professionnels doivent être formés pour sécuriser ces technologies émergentes.

La formation continue doit bénéficier aussi à certaines catégories de professionnels qui, bien qu'ils ne soient traditionnellement associés au domaine de la cybersécurité, sont confrontés à des enjeux liés à l'exercice de leurs métiers. Il s'agit, en l'occurrence, des diplomates œuvrant à la promotion de l'agenda marocain de la cybersécurité au niveau international, des juges et avocats qui traitent des affaires de cybercriminalité ou encore des personnels des organes en charge de l'application de la loi.

► **Adapter l'offre de formations en cybersécurité aux besoins métiers**

Disposer d'une cartographie claire des métiers de la cybersécurité, ainsi que des besoins du marché en la matière, constitue un pilier essentiel pour le développement et la gestion efficace des ressources humaines dans ce domaine stratégique. Une telle initiative permettrait de mieux comprendre la diversité des compétences requises, des responsabilités associées à chaque

poste, ainsi que des parcours professionnels envisageables. En fournissant une vision holistique du paysage professionnel de la cybersécurité, elle contribuera à orienter les politiques de recrutement, de formation et de développement des talents. De plus, elle facilitera l'identification des lacunes en matière de compétences et des besoins de formation spécifiques, favorisant ainsi une allocation judicieuse des ressources et une meilleure adéquation entre l'offre de compétences et la demande du marché du travail offrant de meilleures opportunités d'évolution professionnelle, y compris des possibilités de réinsertion et de reconversion.

Objectif 3.3 : Soutenir le développement de l'écosystème national de cybersécurité et encourager l'innovation

► **Encourager le développement de l'écosystème de cybersécurité à l'échelle nationale (entrepreneuriat, fonds d'investissements, incubation etc.)**

Favoriser le développement d'un écosystème de cybersécurité à l'échelle nationale est crucial pour renforcer la sécurité numérique du pays, encourager l'innovation et soutenir la croissance. Le développement d'un écosystème de cybersécurité robuste nécessite une approche multidimensionnelle impliquant différents acteurs, de l'éducation à l'entrepreneuriat en passant par la réglementation et les investissements. Cela favorisera la croissance de l'industrie de la cybersécurité, la création d'emplois et la protection des infrastructures numériques nationales.

L'objectif est de soutenir l'entrepreneuriat dans ce domaine par la création d'incubateurs et d'accélérateurs dédiés à la cybersécurité et aider les start-up et les entrepreneurs qui développent des solutions innovantes en matière de sécurité. Cela devrait comprendre également la mise à disposition d'espaces de coworking, de mentorat ou de ressources aux jeunes entreprises en cybersécurité.

L'écosystème gagnerait aussi à être développé via l'adoption d'instruments favorables à l'innovation en cybersécurité, comme les systèmes de subventionnement et les fonds d'investissement spécifiques à la cybersécurité, établis pour soutenir la création et la croissance des start-up et des entreprises.

► **Soutenir la recherche et développement au sein des universités et des centres de formation marocains**

Soutenir la recherche et le développement en cybersécurité au sein des universités et des centres de formation est essentiel pour promouvoir l'innovation, renforcer les connaissances et créer un vivier de professionnels qualifiés.

Le soutien de la R&D doit être envisagé par la mise en place de subventions de recherche spécifiques à la cybersécurité pour les professeurs et les chercheurs et aussi par des bourses de recherche et de développement pour les étudiants qui souhaitent se spécialiser en cybersécurité.

Il convient aussi de mettre en place des laboratoires dédiés à la cybersécurité avec pour objectif de produire des travaux permettant de développer de nouvelles méthodes et technologies nationales et d'encourager les chercheurs et les étudiants à déposer des brevets.

La collaboration avec l'industrie est un axe qu'il faut également investir, et ce en établissant des partenariats entre les entreprises et les acteurs industriels pour soutenir la recherche conjointe, les stages et les projets communs.





PILIER 4

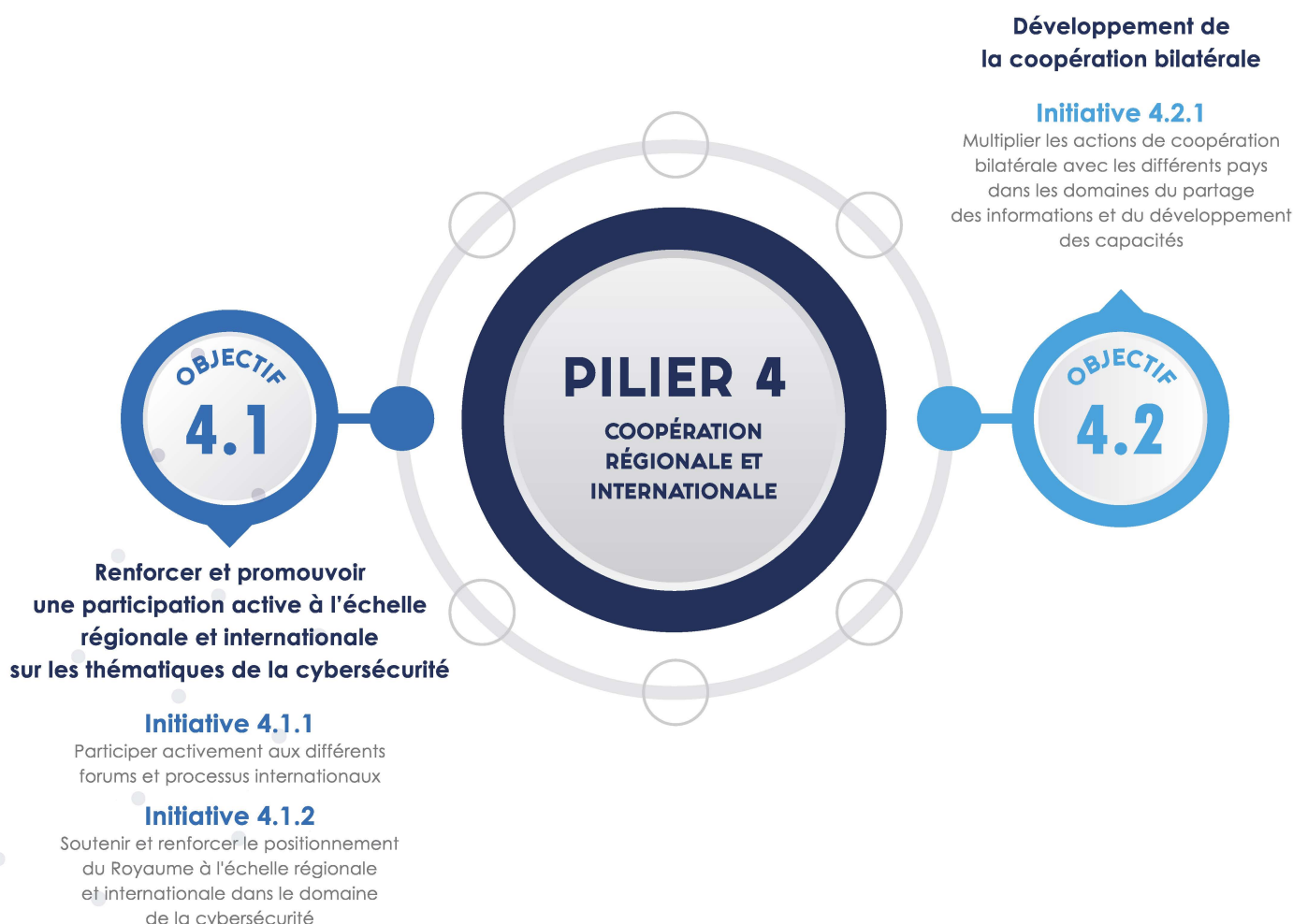


Coopération régionale et internationale

Cette caractéristique transfrontalière et universelle du cyberspace est l'une de ses forces, mais elle présente également des défis en matière de cybersécurité. En effet, le cyberspace n'a pas de frontières physiques, ce qui rend difficile l'application des lois et des réglementations nationales.

Pour cette raison, le renforcement de la coopération internationale, qu'elle soit bilatérale ou multilatérale, s'impose comme un choix stratégique. L'objectif étant de mettre en place un cadre convenu, des mécanismes de coopération et des normes de sécurité à respecter par les pays pour maintenir la paix et la sécurité dans le cyberspace. En travaillant de manière coordonnée, les pays sont en mesure d'échanger des informations sur les menaces et les risques et d'améliorer l'efficacité de leurs dispositifs de prévention et de réponse aux incidents.

Sans aucun doute, l'engagement de notre pays dans les enceintes internationales et la multiplication des initiatives multilatérales ne peut que renforcer notre posture dans le domaine de la cybersécurité.





Objectif 4.1 : Renforcer et promouvoir une participation active à l'échelle régionale et internationale sur les thématiques de la cybersécurité


► **Participer activement aux différents forums et processus internationaux**

Ces dernières années, la cybersécurité est devenue un sujet majeur de débat au niveau international. A ce titre, l'implication de notre pays dans les différents forums et processus internationaux, tels que l'Organisation des Nations Unies, l'Union Africaine, le Global Forum on Cyber Expertise... revêt une dimension cruciale.

En prenant part activement à ces rencontres, le Maroc envisage de contribuer activement aux débats internationaux, notamment celles en rapport avec la construction du cadre normatif international régissant le cyberspace. Les partenariats noués et les opportunités saisies dans le cadre de ces forums internationaux aideront notre pays à renforcer ses capacités nationales et relever les défis croissants afférents à l'espace cybernétique.

► **Soutenir et renforcer le positionnement du Royaume à l'échelle régionale et internationale dans le domaine de la cybersécurité**

Affirmer et consolider le rôle du Royaume du Maroc sur la scène régionale et internationale en matière de cybersécurité constitue un enjeu de taille. Il s'agit de mettre en lumière la vigueur des efforts déployés par le pays dans ce domaine, et ce afin d'asseoir sa légitimité en tant qu'acteur régional majeur et influent. A travers cette initiative, notre pays sera en mesure de contribuer de manière substantielle aux échanges sur la sécurité numérique mondiale, tout en renforçant ses propres compétences et en bénéficiant des synergies découlant des partenariats internationaux.



Pour atteindre cet objectif ambitieux, le pays compte établir des partenariats stratégiques et à partager ses connaissances et son expertise, favorisant ainsi la coopération régionale et internationale.

Objectif 4.2 : Développement de la coopération bilatérale

► Multiplier les actions de coopération bilatérale avec les différents pays dans les domaines du partage des informations et du développement des capacités

Les initiatives de coopération bilatérales marquent à leur tour l'engagement des Etats vis à vis des questions du cyberspace.

Dans ce sens, la présence du Maroc sur la scène internationale doit être accompagnée par un effort soutenu en matière de coopération bilatérale avec les autres pays. Cette coopération bilatérale, de par son caractère complémentaire, est d'une importance cruciale notamment dans les domaines du partage d'informations et du renforcement des capacités en matière de cybersécurité.

L'ouverture sur les autres pays passe par la mise en place d'une collaboration étroite notamment avec les agences nationales en charge de la cybersécurité, les CERTs Dans un esprit de partenariat et de partage, le Maroc pourra ainsi bénéficier d'un échange d'expertise et d'un soutien mutuel, tout en contribuant activement au renforcement de la sécurité numérique à l'échelle mondiale. Par le biais de ces coopérations, notre pays entend tirer des bénéfices tangibles, tels que l'amélioration de sa préparation face aux menaces cybernétiques, l'accès à des ressources et à des connaissances partagées ainsi que la consolidation de sa position en tant qu'acteur de la cybersécurité au niveau régional.



SUIVI ET EVALUATION

La stratégie nationale de cybersécurité établit les grandes orientations stratégiques nationales dans ce domaine à l'horizon 2030. Elle est appuyée par un plan d'actions qui traduit les objectifs de cette stratégie, permettant la concrétisation de la vision du Royaume.

La mise en œuvre de ce plan d'actions est une responsabilité partagée entre les différents acteurs. En parallèle, la responsabilité du suivi incombe à la Direction Générale de la Sécurité des Systèmes d'Information, en sa qualité d'autorité nationale en charge de la cybersécurité.

Dans ce cadre, un tableau de bord de suivi et des bilans périodiques seront dressés afin d'éclairer sur la progression de la mise en œuvre de la stratégie. Ces bilans mettront en relief l'état d'avancement des projets, les résultats obtenus, les enseignements tirés et les éventuelles difficultés rencontrées lors de leur implémentation. Ils constitueront un prérequis indispensable pour permettre au Comité Stratégique de la Cybersécurité de procéder, dans le cadre de ses prérogatives, à des évaluations périodiques pour mesurer les progrès accomplis.

Le suivi/évaluation est une phase cruciale qui détermine le succès de la stratégie. De manière périodique, la stratégie nationale ainsi que le plan d'actions y afférent sont appelés à être revus et mis jour, pour tenir compte des résultats obtenus et aussi de l'évolution du niveau de maturité de notre pays et de l'environnement global des risques et des menaces cybernétiques.



LISTE DES ACRONYMES

CERT : Computer Emergency Response Team

CNDP : Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel

CSC : Comité Stratégique de la Cybersécurité

DGSN : Direction Générale de la Sûreté Nationale

DGSSI : Direction générale de la sécurité des systèmes d'information

DNSSI : Directive Nationale de la Sécurité des Systèmes d'Information

GCI : Global Cybersecurity Index

GR : Gendarmerie Royale

IA : Intelligence artificielle

IdO : Internet des objets

IIV : Infrastructures d'Importance Vitale

maCERT : Centre Marocain de veille, détection et réponse aux attaques informatiques

PMP : Présidence du Ministère Public

SI : Système d'Information

SIS : Systèmes d'Information Sensibles

SNC : Stratégie Nationale de Cybersécurité

SOC : Centre opérationnel de sécurité

UIT : Union Internationale des Télécommunications



DIRECTION GÉNÉRALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Avenue Al Mellia, Hay Ryad, Rabat 10102
www.dgssi.gov.ma
contact-dsr@dgssi.gov.ma

