Agence Monégasque de Sécurité Numérique

Stratégie nationale pour la sécurité du numérique

AMSN · Sécurité Numérique
PRINCIPAUTÉ DE MONACO

www.gouv.mc

La Principauté de Monaco a décidé de s'engager dans la transition numérique. Forte d'une population déjà largement connectée et portée par une économie où le numérique peut être vecteur de croissance, la Principauté de Monaco dispose de talents et d'atouts. Elle a toute sa place dans le concert des nations européennes.

Le numérique devient un espace de compétition et de confrontation. Concurrence déloyale et espionnage, désinformation et propagande, terrorisme et criminalité trouvent dans le cyberespace un nouveau champ d'expression.

La volonté du Gouvernement Princier d'effectuer une transition forte et rapide vers le numérique est l'occasion de promouvoir nos valeurs, notre économie et protéger les personnes. Un cyberespace monégasque sûr, pérenne, de confiance est un gisement de croissance. Monaco doit devenir encore davantage un lieu d'opportunités pour les entreprises.

Notre ambition dans ce domaine doit être forte. Pour ce faire, l'Agence Monégasque de Sécurité Numérique doit être le pivot des actions prévues par la stratégie nationale pour la sécurité du numérique, dont vous trouverez le contenu en annexe.

Cette stratégie s'appuie sur cinq objectifs :

- Assurer la sécurité des infrastructures critiques,
- protéger la vie numérique des personnes et des entreprises et lutter contre la cybercriminalité,
- assurer la sensibilisation et la formation nécessaires à la sécurité du numérique,
- favoriser le développement d'un écosystème favorable à la confiance dans le numérique,
- créer des liens internationaux et améliorer la stabilité du cyberespace.

Elle doit impérativement être portée par l'ensemble de la communauté nationale : le Gouvernement, les entreprises et plus largement, tous les acteurs de la Principauté. La sécurité et la stratégie sont l'affaire de tous.

Répondre aux enjeux de sécurité du monde numérique est un facteur clé de succès collectif. Je souhaite que cette stratégie nationale pour la sécurité du numérique permette de faire de Monaco un pays exemplaire dans ce domaine et compte donc sur votre implication dans la mise en œuvre des plans d'action qui découleront de celle-ci.

Serge Telle
Ministre d'État

Sommaire

STRATÉGIE NATIONALE POUR LA SÉCURITÉ DU NUMÉRIQUE

Introduction

La Principauté de Monaco accomplit sa transition numérique. Les réseaux sont omniprésents dans le fonctionnement de l'État, dans l'activité économique et la vie quotidienne de la population...

Porteur de nouveaux usages, de nouveaux produits et de nouveaux services, le numérique est facteur d'innovation. Il engendre une mutation de la plupart des métiers. Il transforme des secteurs d'activités et des entreprises pour leur apporter plus de souplesse et de compétitivité. Enrichis par l'apport du numérique, ces secteurs sont simultanément plus exposés aux menaces issues du numérique.

Se priver du numérique ou ne pas pouvoir y accéder conduit à une forme d'exclusion économique et sociale. De même, un État qui ne disposerait pas de l'autonomie nécessaire dans le secteur du numérique verrait sa souveraineté menacée.

Pour que le numérique demeure un espace de liberté, d'échanges et de croissance, il est nécessaire que la confiance et la sécurité y soient établies et défendues. Seul un effort collectif et coordonné peut permettre d'atteindre cet objectif.

.....

La Principauté de Monaco a déjà constaté plusieurs incidents de sécurité numérique, il est donc nécessaire d'établir une première stratégie pour la sécurité du numérique.

Les attaques informatiques visent aussi bien les états que les entreprises, de toutes tailles, dans tous les secteurs d'activité. Les entreprises sont également la cible d'escroqueries de toutes sortes comme par exemple l'infection par un logiciel malveillant qui rend les fichiers de l'entreprise inutilisables jusqu'au paiement d'une rançon effectuée par des moyens difficilement traçables.

Parallèlement, les intrusions informatiques destinées à dérober des informations personnelles (identité, données d'identification à des sites marchands, données bancaires) se multiplient. Il s'agit le plus souvent pour des criminels de commettre des délits identiques à ceux connus dans le monde matériel — vols, escroqueries, chantage — mais de manière industrialisée, une part du risque d'être identifié et poursuivi en moins. Le crime organisé s'est saisi de l'avantage procuré par les réseaux de communications électroniques. Ses capacités techniques sont croissantes au point d'être désormais en mesure de pratiquer, pour lui-même ou en sous-traitance par hybridation, des actes de sabotage ou de prise en otage d'outils de production.

Des campagnes de harcèlement se développent sur les réseaux sociaux, comme des cas d'escroqueries aux sentiments destinés à amener les victimes crédules à transférer de l'argent vers l'étranger.

La menace est aujourd'hui certaine et même accentuée par l'accroissement des capacités des attaquants, la prolifération des techniques d'attaques et le développement dans le cyberespace de la criminalité organisée.

Mais un défi d'une autre nature est apparu. Celui de la captation de richesses numériques par un oligopole d'entreprises utilisant leur position dominante pour gêner l'arrivée de nouveaux entrants et capter la valeur ajoutée de cette économie naissante qui exploitera les données pour inventer de nouveaux services, améliorer notre vie quotidienne ou rendre plus accessibles les services publics. Parmi ces données figurent au premier plan nos données personnelles, y compris celles relatives à notre vie privée. La maîtrise de ces masses de données ouvre la voie à la déstabilisation économique et à des formes sophistiquées de propagande ou d'orientation des convictions ou des habitudes.

.....

L'Organisation des Nations Unies (ONU) a reconnu en 2013 l'application au cyberespace du droit international.

.....

Alors qu'émerge une société massivement connectée, la responsabilité de la sécurité numérique doit désormais être partagée par l'ensemble des personnes résidant ou travaillant en Principauté. Un objet connecté ou un service insuffisamment sécurisé par ses développeurs, la négligence d'un décideur en matière de sécurité des systèmes d'information, le comportement dangereux d'un prestataire ou celui d'un salarié mélangeant sans précaution vie privée et vie professionnelle peuvent entraîner pertes de disponibilité, de confidentialité ou d'intégrité d'informations essentielles, ruptures d'activité et pertes économiques, accidents industriels et pertes de vies humaines ou catastrophes écologiques et troubles à l'ordre public, susceptibles d'affecter la vie de la Principauté de Monaco.

Jamais, en effet, la stabilité de notre avenir, porté par le numérique, n'a été aussi dépendante des responsabilités de chacun et de celles, collectives, de trois communautés d'acteurs.

La première communauté a la responsabilité de proposer et de mettre en œuvre des technologies, des produits et des services dotés du niveau de sécurité adapté aux usages et capables de parer les risques identifiés. Les principaux acteurs de cette communauté sont les inventeurs et fournisseurs de produits et services et leurs intégrateurs, les opérateurs de réseaux de communications électroniques, les fournisseurs d'accès à internet ou les fournisseurs de services informatiques distants.

La deuxième communauté a pour responsabilité de protéger la Principauté de Monaco des prédateurs du numérique. Outre la mise en œuvre des politiques de cybersécurité, il s'agit notamment de conduire de façon volontariste une politique de développement des compétences techniques nécessaires et de mettre en place un écosystème de confiance qui accompagne la transformation numérique de la société, en défendant les personnes, nos valeurs et nos intérêts dans le cyberespace. Cette responsabilité engage celui qui la porte à exprimer sa position en faveur de solutions de sécurité. Cette communauté est constituée des élus, du Gouvernement, des administrations.

La troisième communauté a pour responsabilité d'utiliser de manière réfléchie les services et technologies disponibles, d'effectuer des choix raisonnés et d'éviter les comportements à risque dans les actes de la vie numérique. Cette communauté est constituée de tous les usagers, responsables d'entreprises, acteurs de la société civile et particuliers.

L'État a pour rôle dans le cyberespace (le garantir la liberté d'expression et d'action de la Principauté de Monaco et d'assurer la sécurité de ses infrastructures critiques en cas d'attaque informatique majeure (objectif 1), de protéger la vie numérique du grand public et des entreprises, de lutter contre la cybercriminalité (objectif 2), d'assurer la sensibilisation et la formation nécessaires à la sécurité du numérique (objectif 3), de favoriser le développement d'un écosystème favorable à la confiance dans le numérique (objectif 4), de créer des liens internationaux et améliorer la stabilité du cyberespace (objectif 5).

5 objectifs stratégiques

objectif 1

Intérêts fondamentaux,
défense et sécurité
des systèmes d'information
des institutions officielles
de la Principauté
et des infrastructures
critiques, crises
informatiques majeures

Enjeux

La Principauté de Monaco est la cible d'attaques informatiques qui portent atteinte à ses intérêts fondamentaux.

Aujourd'hui, lorsqu'un attaquant cible des institutions officielles de la Principauté, les opérateurs d'importance vitale ou des entreprises, il cherche à s'installer durablement dans le système d'information visé pour y voler des données confidentielles (politiques, diplomatiques, technologiques, économiques, financières ou commerciales).

Demain, un attaquant pourrait prendre le contrôle d'objets connectés, interrompre à distance une activité industrielle ou économique ou détruire sa cible.

Parallèlement, des attaques informatiques destinées à frapper l'opinion publique sont fréquentes, à titre d'exemple, les défigurations de sites internet qui ont eu un impact technique faible mais une portée symbolique souhaitée par les attaquants.

Depuis plusieurs années, plusieurs États ont mis en œuvre leur volonté politique et des moyens humains, techniques et financiers considérables afin de mener des opérations informatiques à grande échelle dans le cyberespace.

Qu'elles soient connues par des documents publiquement révélés ou mis en évidence lors du traitement d'attaques informatiques, les excès de telles pratiques entament la crédibilité de certains de ces États sur la scène internationale.

Objectif

La Principauté de Monaco se donnera les moyens de défendre ses intérêts fondamentaux dans le cyberespace. Elle consolidera la sécurité numérique de ses infrastructures critiques et œuvrera pour celle de ses opérateurs d'importance vitale.

A ce titre, il a été créé par l'Ordonnance Souveraine n°5.664 du 23 décembre 2015 une autorité administrative dénommée l'Agence Monégasque de Sécurité Numérique placée sous l'autorité du Conseiller de Gouvernement - Ministre de l'intérieur.

L'Agence Monégasque de Sécurité Numérique est l'autorité nationale en charge de la sécurité des systèmes d'information.

Pour autant des orientations complémentaires seront nécessaires.

Orientations

- *Détenir les capacités internes, ou sous-traitées à des tiers de confiance, nécessaires à la protection de l'information de souveraineté, à la cybersécurité et au développement d'une économie numérique de confiance.*

Un comité stratégique pour la sécurité numérique sera créé, sous l'égide du Ministre d'État, l'Agence Monégasque de Sécurité Numérique en assure le secrétariat.

Le comité stratégique pour la sécurité numérique réunira très régulièrement les administrations compétentes de la Principauté de Monaco (éducation, justice, affaires sociales, santé, intérieur, économie, scientifique et recherche, direction du travail, etc.). Le comité pourra associer à ses travaux des autorités administratives indépendantes, des acteurs du secteur privé et des personnalités qualifiées.

La mission de ce groupe sera notamment de suivre les plans d'action découlant de la présente stratégie, d'identifier les technologies-clés pour le développement d'un environnement numérique de confiance. Il évaluera les besoins en formations initiales et continues, suivra les travaux de recherche et en accompagnera la valorisation.

Le comité pour la sécurité numérique organisera la veille technologique et économique permettant d'anticiper les évolutions des questions liées au numérique. Le cas échéant, des mesures adaptées seront proposées pour accompagner ou cadrer ces évolutions.

- *Assurer au profit des institutions officielles de la Principauté, des entreprises et du grand public une veille active en matière de sécurité des technologies et des usages.*

Dans la perspective d'évolutions technologiques majeures, comme les télécommunications mobiles de 5e génération (5G) ou les « réseaux définis par le logiciel », la Principauté de Monaco restera vigilante sur la nature et les capacités des équipements matériels et logiciels installés au cœur de ses réseaux de communications électroniques, pour protéger le secret des correspondances, la vie privée et la résilience de ces infrastructures, et poursuivra l'adaptation de son cadre réglementaire aux nouvelles technologies émergentes.

L'Agence Monégasque de Sécurité Numérique informera régulièrement les institutions officielles de la Principauté, les entreprises, et le grand public, par des moyens adaptés au public visé, des éléments susceptibles de présenter un danger dans leur utilisation du numérique. Le cas échéant, ces informations auront, au préalable, été consolidées avec les administrations compétentes.

- *Accélérer le renforcement de la sécurité des systèmes d'information des institutions officielles de la Principauté.*

Afin de traiter les informations soumises au secret de sécurité nationale, la Principauté se dotera des moyens de télécommunications et informatiques nécessaires.

Une politique de sécurité des systèmes d'information de l'État (PSSIE) sera élaborée, le déploiement de terminaux mobiles sécurisés a été initié et sera poursuivi. Ces actions mobilisent des ressources humaines et budgétaires qu'il sera nécessaire de dimensionner et d'adapter.

L'application de la politique de sécurité des systèmes d'information de l'État et l'efficacité des mesures adoptées seront évaluées annuellement. Un bilan annuel confidentiel sera transmis au Ministre d'État et le Conseil National sera informé.

Pour tous projets ou propositions de loi, une étude d'impact (financier et technique) sur le numérique et la cybersécurité sera effectuée dès 2017.

- *Préparer la Principauté de Monaco à faire face à une crise informatique majeure.*

Le renforcement de la sécurité du numérique des opérateurs d'importance vitale fait l'objet de mesures législatives (Loi n°1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique) adoptée par le Conseil National en séance publique le 27 octobre 2016. Les travaux devront être engagés avec ces opérateurs dès que possible et poursuivis durablement.

La Principauté de Monaco mettra en place au plus tard avant fin 2017 un CERT-MC reconnu par la communauté internationale. Centre de veille, d'alerte et de réponse le CERT-MC, est au sein de l'Agence Monégasque de Sécurité Numérique, responsable de la prévention, de la détection et du traitement des cyberattaques sur les systèmes d'information.

Des exercices de gestion de crise cybernétique seront menés dès 2018 et concerneront progressivement l'ensemble des opérateurs d'importance vitale et les partenaires internationaux.

objectif 2

Confiance numérique,
vie privée,
données personnelles,
cyber malveillance

Enjeux

S'ils ont de manière générale confiance dans le numérique, les personnes ont, en revanche, une certaine défiance quant à son impact sur leur vie quotidienne, notamment personnelle. Généralement soucieux de l'utilisation et de la conservation de leurs données personnelles, ils les confient toutefois à des plates-formes dont les conditions d'utilisation sont léonines au détriment des utilisateurs.

Le mode opératoire constaté lors de certaines attaques informatiques contre des entreprises ou des administrations montre également une réelle difficulté à dissocier vie privée et vie professionnelle dans l'utilisation des équipements comme des services.

Les attaques informatiques qui touchent les particuliers ont généralement pour objectif le gain financier. Par la prise de contrôle de l'équipement personnel utilisé — ordinateurs, tablettes, ordiphones —, l'usurpation d'identité et le vol d'identifiants à des comptes bancaires ou à des sites commerciaux, par l'engagement d'une relation affective virtuelle débouchant sur une demande de transfert d'argent, par le chiffrement de données à l'insu de l'utilisateur conduisant au paiement d'une rançon, le racket est aujourd'hui pratiqué à grande échelle par une criminalité qui s'est organisée et a gagné en efficacité.

Bien qu'il ne fasse appel à aucune technique d'attaque particulière, le harcèlement, facilité et amplifié par les réseaux de communications électroniques, est une agression informatique contre les personnes dont l'issue est parfois dramatique.

Si l'Agence Monégasque de Sécurité Numérique est l'interlocuteur étatique identifié en cas d'incident informatique grave affectant les administrations et les opérateurs d'importance vitale, la lisibilité de l'offre publique est nettement moindre en matière d'assistance aux victimes d'actes de cyber malveillance pour les autres acteurs, qu'il s'agisse d'entreprises de taille intermédiaire, de petites et moyennes entreprises, de professions libérales ou de particuliers.

Les victimes d'actes de cyber malveillance sont encouragées à déposer une plainte, auprès des services de police qui ne sont pas forcément adaptés au traitement de tels contentieux. Toutefois, la réponse qui leur est apportée dans ce cadre est centrée sur l'identification des auteurs présumés de La cyber malveillance et sur l'engagement éventuel de poursuites contre ces auteurs. Les victimes doivent pouvoir être orientées vers un service d'assistance au traitement de l'incident informatique à l'origine de l'acte de cyber malveillance.

Plus insidieusement, les plateformes numériques et notamment les réseaux sociaux façonnent l'opinion et sont vecteurs de valeurs qui parfois ne sont pas celles de La Principauté. Dans certains cas, ils peuvent être instrumentalisés à des fins de désinformation et de propagande envers le grand public, notamment les plus jeunes. **Dans certains cas, les opinions diffusées vont à l'encontre des intérêts fondamentaux de la Principauté de Monaco et relèvent alors d'une atteinte à la sécurité nationale sanctionnée par la loi.**

Dans un registre différent, les développements récents et simultanés de nouveaux usages et de nouvelles techniques de stockage et de traitement des données favorisent l'émergence de risques de déséquilibre économique et d'atteinte à la sécurité individuelle des personnes ainsi qu'à celle des nations.

Le souhait de voir instaurer, par exemple aux travers de traités commerciaux, la libre circulation des données, dont les données personnelles collectées par des objets connectés, masque difficilement la volonté de captation de ces données par des oligopoles dont les valeurs et les pratiques ne correspondent ni à la conception de la vie privée en Principauté ni à son encadrement juridique. La captation massive et illicite de certains types de données personnelles, comme par exemple les données de santé, peut en effet entraîner des atteintes à la sécurité individuelle et collective, ou plus simplement une exploitation commerciale abusive (revente à des compagnies d'assurance, par exemple).

Le développement numérique ne peut être durable dans un cyberespace où les États ne respectent pas les bonnes pratiques nécessaires à une transition numérique équilibrée et profitable à toutes les nations et où quelques acteurs économiques s'accaparent la richesse que constituent les données numériques, notamment les données personnelles, véritables ressources des générations futures.

Objectif

La Principauté de Monaco développera un usage du cyberespace conforme à ses valeurs et y protègera la vie numérique des particuliers. Elle accroîtra sa lutte contre la cybercriminalité et l'assistance aux victimes d'actes de cyber malveillance.

Orientations

- *Promouvoir et défendre nos valeurs sur les réseaux de communications électroniques et dans les instances internationales.*

Les droits des personnes s'appliquent de la même manière « en ligne » et « hors ligne ». Le cyberespace doit ainsi rester un lieu de libre expression pour toute la population, où les abus ne peuvent être prévenus que dans la mesure des limites fixées par la loi et en conformité avec nos engagements internationaux. La Principauté de Monaco promeut cette approche destinée à préserver un cyberespace libre et ouvert dans les instances internationales.

Il appartient à l'État d'informer la population sur les risques de manipulation et les techniques de propagande utilisées par des acteurs malveillants sur Internet. Le Gouvernement mettra en place une plate-forme d'information sur les risques liés au numérique.

• *Apporter une assistance de proximité aux victimes d'actes de cyber malveillance.*

L'Agence Monégasque de Sécurité Numérique en liaison étroite avec la direction de la Sûreté Publique mettra en place dès 2017 un dispositif destiné à porter assistance aux victimes d'acte de cyber malveillance.

Ce dispositif aura également une mission de sensibilisation aux enjeux de protection de la vie privée numérique et de prévention.

Le dispositif devra proposer aux victimes des solutions s'appuyant sur des acteurs de proximité et faciliter les démarches administratives, notamment afin de favoriser le dépôt de plainte.

• *Mesurer la cybercriminalité.*

Aujourd'hui force est de constater qu'il n'existe pas de statistiques fiables relatives spécifiquement à la délinquance ou à la criminalité informatique.

L'absence de telles statistiques est préjudiciable à la conception par les pouvoirs publics de politiques constamment réévaluées et à la mise en place des moyens adaptés. C'est pourquoi la Direction de la Sûreté Publique mettra en œuvre un suivi de l'évolution de la cybercriminalité afin d'éclairer l'action publique.

• *Protéger la vie numérique, la vie privée et les données personnelles.*

La Principauté de Monaco se dotera d'une feuille de route claire en matière d'identité numérique, authentification et signature. Cette feuille de route, dont l'élaboration a déjà débutée, sera finalisée début de l'année 2017 sous l'égide de la Direction de l'Administration Electronique appuyée par les services compétents.

Cette feuille de route prévoira le déploiement de dispositifs de fédération d'identité permettant d'utiliser une même identité numérique de confiance pour s'authentifier sur différents services.

Pour les usages les plus sensibles, tels que ceux concernant la vie démocratique ou les échanges internationaux relatifs à la justice, des niveaux de confiance élevés dans les dispositifs et services seront systématiquement employés.

La Principauté de Monaco protégera la vie privée et les données personnelles de la population. Les droits à la vie privée et à la maîtrise individuelle et collective des données personnelles seront réaffirmés chaque fois que nécessaire et notamment à l'occasion des négociations commerciales entre États, qu'elles soient bilatérales ou multilatérales.

Pour informer les personnes sur l'utilisation faite des données confiées aux services numériques, une signalétique adaptée et partagée avec les États volontaires et en cohérence avec les travaux européens effectués dans le cadre du règlement européen relatif à la protection des données à caractère personnel sera mise en place courant 2017. Cette signalétique permettra de visualiser les caractéristiques essentielles des conditions d'utilisation des plates-formes et services numériques ou des moyens de paiement utilisés.

objectif 3

Sensibilisation,
formations initiales,
formations continues

Enjeux

La Principauté de Monaco a besoin de sensibiliser sa population aux risques associés aux usages du numérique et de la former à la cybersécurité.

Les personnes négligent en général les bonnes pratiques lors de l'utilisation des réseaux de communications électroniques.

Dans l'usage privé des réseaux de communications électroniques, les enfants et adolescents, confrontés à des contenus inadaptés, exposés au harcèlement ou à la prédation, sont les premières victimes. Afin de rompre le silence et de permettre les poursuites, les plus jeunes devraient être initiés à la conduite à tenir lorsqu'ils sont victimes de malveillance numérique.

La sensibilisation de tous est un préalable nécessaire pour que les élus, les dirigeants d'administrations ou d'entreprises puissent prendre en compte le « risque cyber » à son juste niveau et décider des mesures susceptibles de protéger les personnes qu'ils représentent ou les organismes qu'ils dirigent, face à des menaces de vol d'informations ou de propriété intellectuelle, d'atteinte aux données personnelles, voire l'exposition à des ruptures d'activité, d'accidents de production, avec des impacts technologiques ou environnementaux auxquels ils sont potentiellement exposés.

Outre la sensibilisation des plus jeunes, toutes les formations à tous les métiers doivent permettre aux futurs professionnels de bénéficier d'une sensibilisation plus ou moins importante en sécurité du numérique.

Objectif

La Principauté de Monaco poursuivra et intensifiera, dès l'école primaire, à la sécurité du numérique et aux comportements responsables dans le cyberespace. Les formations initiales supérieures et continues intégreront un volet consacré à la sécurité du numérique adapté à la filière considérée.

Orientations

- *Sensibiliser l'ensemble de la population.*

Un programme ambitieux de sensibilisation de l'ensemble de la population résidant ou travaillant en Principauté doit être engagé.

Sous la conduite de la Direction de l'Education Nationale de la Jeunesse et des Sports avec l'appui de l'Agence Monégasque de Sécurité Numérique, un appel à manifestation d'intérêt pour la réalisation de contenus de sensibilisation à destination du grand public sera poursuivi ou relancé.

Le Département de l'intérieur mettra en place un « Permis Internet ». En cohérence avec les dispositifs déjà existants, cette opération permettra de sensibiliser aux risques et de conseiller les élèves des écoles primaires chaque année pour les protéger dans leur navigation sur internet.

La visibilité du portail (https://www.ccin.mc/publications/) de la Commission de Contrôle des Informations Nominatives (CCIN) sera renforcée.

- *Intégrer la cybercriminalité dans toutes les formations initiales ou continues.*

La Direction de l'Education Nationale de la Jeunesse et des Sports avec la Direction du travail incitera à ce que, dès la rentrée 2017, des sensibilisations à la cybersécurité correspondant à la filière de formation soient mises en place dans toute formation initiale, continue ou supérieure.

objectif 4

Faire de la sécurité
du numérique
un facteur
de compétitivité
et de confiance

Enjeux

Le cyberespace est en construction rapide. Dans le monde 100 000 objets nouveaux se connectent chaque heure à internet.

Les grands équipements qui assurent le fonctionnement des réseaux de communications électroniques dont les infrastructures sont situés en Principauté de Monaco, sont souvent conçus, développés et parfois administrés depuis des centres situés hors de l'Europe. Il en est de même pour l'essentiel des équipements de communications et de sécurité informatique de nos opérateurs d'importance vitale. Le fonctionnement d'un nombre croissant d'entreprises repose sur l'utilisation d'applications et le traitement de données hébergés dans des espaces immatériels non maîtrisés, portés par des infrastructures physiques situées hors du territoire et non soumises au droit monégasque et souvent européen.

Les évolutions en cours tant au niveau des technologies que dans les modèles économiques, avec par exemple la multiplication des objets connectés ou la concentration des plateformes de service en ligne entre les mains de quelques acteurs seulement, sont de nature à amplifier cette perte de maîtrise du cyberespace national. En cas de crise internationale, l'accès à des pans entiers du cyberespace pourrait nous être contesté.

La réponse à cet enjeu de souveraineté nécessite une offre d'équipements et de services numériques qui apportent à leurs clients les garanties de sécurité et de confiance adaptées aux enjeux et aux usages.

Les utilisateurs n'ont pas le moyen de s'assurer eux-mêmes du niveau de sécurité des objets et services numériques. La promotion de la sécurité dans le discours commercial des fournisseurs se généralise sans toutefois permettre une évaluation objective du niveau de sécurité réellement atteint. Le développement d'une plus grande lisibilité sur le plan de la sécurité de l'offre numérique, fondée sur des éléments objectifs et vérifiables par un tiers, constitue un défi majeur pour assurer la confiance dans l'économie numérique.

Le défi posé aux entreprises monégasques est de concilier recherche de productivité, d'économies, de rentabilité et utilisation ou développement de produits et services numériques ne mettant pas en danger leur compétitivité ou leur sécurité, celles de leurs partenaires ou celles de leurs clients.

La plupart des équipements, objets et services numériques disponibles aujourd'hui sur le marché n'ont pas le niveau de sécurité informatique leur permettant d'éviter un incident — fuite de données, dysfonctionnement ou rupture de service.

Objectif

La Principauté de Monaco fera de la sécurité du numérique un facteur de compétitivité. Elle s'assurera de la disponibilité pour le grand public, les entreprises et les institutions officielles de la Principauté, de produits et services numériques présentant des niveaux d'ergonomie, de confiance et de sécurité adaptés aux usages et aux cyber menaces.

Orientations

- *Faire connaître et valoriser l'offre de produits et services de sécurité.*

Dès fin 2016, l'Agence Monégasque de Sécurité Numérique établira une liste de matériel et de services de confiance puis accentuera ses efforts en matière de qualification et de suivi de produits et de services de sécurité informatique.

En lien avec les administrations compétentes, l'Agence Monégasque de Sécurité Numérique engagera en 2017 une information sur les produits et services de sécurité informatique de confiance.

- *Assurer la capacité de prévenir, détecter et traiter les attaques informatiques pour les institutions officielles et les OIV.*

La Principauté de Monaco se dote d'une capacité de détection et de traitement des attaques informatiques par le biais de l'Agence Monégasque de Sécurité Numérique. Cet effort devra être poursuivi, mais il appartient aux OIV d'assurer leur propre sécurité dans le domaine informatique, l'Agence Monégasque de Sécurité Numérique ne devant intervenir que pour du conseil, du contrôle ou en cas de crise.

- *Préparer un monde numérique plus sûr par une meilleure anticipation des usages, un accompagnement adapté et une information des acteurs.*

Pour les cinq ans à venir, la priorité des administrations et des OIV pour la sécurité du numérique doit être l'anticipation et la prévention.

Il s'agira d'obtenir que les produits et services numériques ou intégrant du numérique, conçus, développés et mis en place en Principauté de Monaco, soient parmi les plus sûrs au monde.

Lorsque les produits et services numériques hébergeront des données personnelles ou seront destinés aux secteurs d'activité d'importance vitale, l'Agence Monégasque de Sécurité Numérique apportera les éléments utiles à l'analyse des risques ou les conseils nécessaires à l'obtention du niveau de sécurité correspondant à l'usage du produit ou du service en cours de conception ou de développement. Elle contribuera également, pour les usages qui le justifient, à mettre en place des dispositifs permettant d'évaluer de manière indépendante le niveau de sécurité et de confiance de ces produits et services, et d'offrir à leurs utilisateurs potentiels des garanties adaptées par le biais d'une labellisation.

Parallèlement, l'environnement juridique d'accueil des nouveaux produits et services devra être anticipé. À titre d'exemple, la prochaine arrivée de véhicules autonomes doit inciter le régulateur à préparer les conditions assurant la sécurité de leur circulation. La cybersécurité doit être prise en compte dès à présent en définissant le référentiel et les procédures techniques de contrôle.

Pour d'autres types de produits ou services, une signalétique adaptée devra informer le consommateur de leurs caractéristiques numériques essentielles et notamment du traitement qui est réalisé des données collectées. Pour certains secteurs, comme celui de la santé, une labellisation systématique des produits et services numériques sera étudiée.

La Principauté de Monaco cherchera à s'associer à d'autres États pour la mise en œuvre de ces pratiques afin de créer une zone de confiance et de sécurité numériques.

- *Intégrer l'exigence de cybersécurité dans la commande et le soutien publics.*

Pour la protection de sa souveraineté et notamment la protection de ses informations relevant du secret, la Principauté de Monaco conservera une capacité financière à la mise en place des solutions atteignant les justes niveaux de sécurité.

Plus généralement, l'ensemble de l'administration devra démontrer son exemplarité dans le cadre de la commande publique, en intégrant des critères de cyber sécurité au juste niveau dans ses choix des produits et services numériques.

Enfin, dès 2017, tout produit ou service embarquant ou s'appuyant sur un système d'information et souhaitant répondre à un appel d'offres, à un appel à projet publics, ou accéder à des fonds publics bénéficiera d'un facteur de bonification s'il est accompagné d'une analyse de risque en matière de cybersécurité correspondant à l'usage prévu du produit ou service et de la réponse technique apportée.

objectif 5

Liens internationaux, stabilité du cyberespace

Enjeux

Le cyberespace est devenu un sujet majeur de négociation au sein des organisations internationales dont les travaux portent désormais sur l'ensemble du champ du numérique.

En 2013, les États ont reconnu que loin d'être d'un espace sans règle, le cyberespace était régi par le droit international existant. Pour autant, le cadre normatif international est encore en débat, ce qui, en l'absence d'avancée des négociations, pourrait nuire à la préservation d'un cyberespace stable et sûr, respectueux des droits fondamentaux et propice au développement d'une économie prospère et de confiance à l'ère numérique.

Tandis qu'un nombre croissant de pays déclarent se doter de capacités offensives, la conflictualité entre États trouve à s'exprimer de manière croissante dans le cyberespace. Par ailleurs, les révélations de pratiques massives et de techniques d'espionnage menées par de grands États ou des alliances d'États contre d'autres — parfois alliés —, des personnes et des entreprises, ont accru la défiance politique contre les pays à l'origine de ces pratiques et la méfiance technique vis-à-vis de leurs produits et services. Ces révélations favorisent aussi la prolifération de moyens techniques similaires.

Parallèlement, des groupes d'individus aux motivations et soutiens divers, mercenaires recrutés mondialement et associés au gré des circonstances, recourent régulièrement à des attaques informatiques dans le cyberespace pour tenter de déstabiliser les autorités gouvernementales de nombreux pays ou des entreprises qui les incarnent symboliquement. Des organisations terroristes profitent par ailleurs de l'audience portée par les réseaux sociaux pour diffuser une propagande destinée à attirer des volontaires et terroriser des populations. Ces différents groupes bénéficient d'un impact médiatique constant.

Sur le plan économique, la tendance du début de la décennie se confirme. Un petit nombre d'entreprises, portées par les États qui ont permis leur développement, utilisent leur avance technologique, leur domination sur le marché et leurs capacités financières pour préempter l'innovation numérique. Cette privatisation du cyberespace au profit de quelques monopoles condamne les autres acteurs du numérique à la dépendance et capte une part trop importante de la valeur ajoutée du numérique pour que cette situation soit supportable par les économies des autres pays.

S'il porte la croissance du monde, le cyberespace est devenu un lieu de compétition souvent déloyale et de conflits, jusqu'à présent de basse intensité informatique, de déstabilisation politique et d'hégémonie économique.

L'Europe a su identifier ces enjeux et tente d'apporter par le discours et la réglementation des idées et des solutions plus respectueuses d'un développement numérique durable, tant en matière de gouvernance d'internet que de protection des données personnelles ou de sécurité informatique des opérateurs essentiels à l'économie.

Parce qu'elle partage des valeurs communes avec d'autres États-membres de l'Union européenne, la Principauté de Monaco doit y avoir avec eux un rôle en matière de numérique.

La Principauté de Monaco veut participer à la transformation numérique de l'Europe par des alliances. L'Europe s'est construite hier par une alliance autour de matières premières. L'Europe numérique se construira sur des alliances, de la confiance et la maîtrise des données, matières premières des prochaines décennies.

Objectif

La Principauté de Monaco, dans quelques années, lorsqu'elle aura atteint un niveau suffisant dans ce domaine, sera un acteur pour la promotion d'un cyberespace sûr, stable et ouvert en Europe.

Orientations

- *Établir avec les États volontaires une feuille de route pour la promotion d'un cyberespace sûr et stable.*

Ouverte aux États volontaires, cette feuille de route à termes déterminera les facteurs-clés de succès de la mise en place des politiques propices à l'émergence d'un espace numérique stable et compréhensible par tous notamment en matière de réglementation, de normalisation et de certification, de confiance dans le numérique, de sécurité du numérique — en veillant au respect de la souveraineté des États-membres, de protection de la vie privée et des données personnelles conçues comme un bien d'intérêt public.

- *Renforcer la présence et l'influence de la Principauté dans les discussions internationales sur la cybersécurité.*

Afin de renforcer la confiance à l'échelle internationale et d'explorer de nouveaux mécanismes de régulation visant à prévenir les conflits dans le cyberespace, la Principauté de Monaco, dès que le niveau atteint sera satisfaisant, renforcera ses contacts avec toutes les parties prenantes disposées à engager le dialogue sur les enjeux de cybersécurité.

La participation aux négociations multilatérales sur la cybersécurité (ONU, OSCE) sera, alors, accentuée afin de consolider un socle global d'engagements de bonne conduite pour les États dans le cyberespace, dans le respect du droit international.

Les contacts bilatéraux doivent permettre de faire progresser la Principauté en se conformant aux bonnes pratiques et, par ce moyen, de rapidement parvenir à un standard conforme aux normes internationales afin de permettre à la Principauté de jouer un rôle sur la scène internationale.

Afin d'assurer la durabilité et la soutenabilité des projets de renforcement de ses capacités, la Principauté de Monaco inscrira de préférence son action dans des partenariats de confiance à long terme.

Agence Monégasque de Sécurité Numérique

24, rue du Gabian
MC 98000 MONACO
Tél : + 377 98 98 24 93
www.gouv.mc

Gouvernement Princier
PRINCIPAUTÉ DE MONACO