GUIDE PRATIQUE

GUIDE PRATIQUE DE LA CYBERSÉCURITÉ ET DE LA CYBERDÉFENSE

ORGANISATION INTERNATIONALE DE la francophonie

La cybersécurité et la cyberdéfense

GUIDE PRATIQUE

« L'Organisation internationale de la Francophonie souhaite remercier Madame la professeure Solange Ghernaouti de l'université de Lausanne pour sa contribution majeure à l'élaboration de ce document, comme experte principale qui a dirigé l'équipe de rédaction du Guide, et à M. Jacques P. Houngbo d'AfricaCERT qui a proposé le premier jet, ainsi que tous les participants à la Conférence internationale sur le renforcement de la cybersécurité et de la cyberdéfense dans l'espace francophone (Grand-Bassam, Côte d'Ivoire, 8 au 10 février 2016). »

Sommaire

Préface

Les chefs d'État et de gouvernement, réunis au XVIe Sommet de la Francophonie à Antananarivo (Madagascar), les 26 et 27 novembre 2016 ont, dans leur Déclaration finale, salué les actions entreprises par la Secrétaire générale dans le cadre de la mise en œuvre de la Stratégie numérique (Kinshasa, 2012).

Les États et gouvernements de la Francophonie ont encouragé l'Organisation internationale de la Francophonie (OIF) à « poursuivre ses efforts pour accompagner les États et gouvernements membres dans leur volonté d'instaurer un environnement de confiance numérique, dans le respect des droits fondamentaux des personnes, notamment le respect de la vie privée, de la liberté d'expression et la protection des données à caractère personnel ».

Le Guide pratique de la cybersécurité et de la cyberdéfense, que vous avez entre les mains, est une première réponse à cette exhortation des chefs d'État et de gouvernement qui réaffirme la vision de la Francophonie dans le domaine de la sécurité numérique. Cette vision exprime sans ambages l'attachement de la Francophonie à un équilibre entre la liberté et la sécurité dans un contexte de construction d'un écosystème de confiance, et avec l'objectif de favoriser le développement de l'économie numérique et l'épanouissement de la diversité culturelle et linguistique.

Imprégné de cette vision, ce Guide propose de prendre en considération les principaux impacts des cyberrisques sur les personnes, les entreprises et l'État avant d'établir un plan d'action. Ce plan doit partir de l'analyse les risques et mesures de sécurité dans le respect des droits fondamentaux de la protection des données à caractère personnel et d'un cadre juridique encadrant l'intervention des différents acteurs de la cybersécurité pour générer une stratégie nationale de cybersécurité et de cyberdéfense. Il en ressort un continuum entre la cybersécurité et la cyberdéfense que les pays doivent prendre en compte pour assurer l'efficacité de leur action. Mais, cette action ne peut produire des effets profitables que si la question centrale du renforcement des capacités et du capital humain est réglée de façon durable.

Ce guide se décline donc comme une boîte à outils que l'OIF propose aux États et gouvernements pour les accompagner dans leurs efforts pour répondre aux menaces et vulnérabilités des technologies de l'information et de la communication dont toutes nos sociétés et nos économies sont de plus en plus dépendantes.

En proposant un tel instrument, l'OIF met en œuvre l'une des conclusions de la Conférence sur le renforcement de la cybersécurité et la cyberdéfense dans l'espace francophone (Grand-Bassam, Côte d'Ivoire, 8-10 février 2016). Je tiens à remercier Madame la professeure Solange Ghernaouti, de l'université de Lausanne pour sa contribution majeure à l'élaboration de ce document, comme experte principale qui a dirigé l'équipe de rédaction du Guide, ainsi que Monsieur Jacques Houngbo d'AfricaCERT qui a esquissé le document de base de la conférence de la Grand-Bassam.

Je forme le vœu que ce Guide pratique puisse constituer une boussole pour notre action commune à toutes et tous en faveur du renforcement de la cybersécurité et de la cyberdéfense au sein de la Francophonie.

Adama OUANE
Administrateur
de l'Organisation internationale
de la Francophonie

Résumé

Les technologies de l'information et de la communication deviennent indissociables de toutes nos activités et sont en passe de devenir des facteurs structurants civilisationnels. Toutefois, les infrastructures et services issus du numérique, ainsi que les caractéristiques d'Internet, favorisent l'expression de la criminalité et étendent les possibilités et les opportunités criminelles.

Ces dernières années ont été le témoin de l'essor de cyberincidents affectant, à divers degrés, tout un chacun. Qu'il s'agisse d'incivilité, de harcèlement, d'escroquerie, de fraude, de vol, de destruction, de dysfonctionnement, de surveillance, d'espionnage, d'activisme ou encore par exemple de terrorisme ou de désinformation, toute forme de délit, de violence ou de conflictualité se matérialise via l'Internet.

Comprendre les risques auxquels est exposé l'individu, l'organisation publique et privée, l'État et plus généralement la société permet d'agir. Pour ne pas rester démunis et passifs au regard des problèmes engendrés par des cyberattaques ou le détournement des technologies, les dirigeants politiques et économiques se doivent de s'approprier les fondamentaux de la cybersécurité nécessaire à la maîtrise des risques et au développement harmonieux de l'écosystème numérique.

Toute réponse pragmatique aux besoins de sécurité, de protection et de réaction aux problèmes générés par le numérique, par nos interactions et notre dépendance aux systèmes d'information, au cyberespace et à Internet, se base sur une approche stratégique, qui fixe le cadre d'un plan d'action. Cette vision stratégique est nécessaire pour gouverner, piloter et assurer la cohérence et la complémentarité des mesures stratégiques et opérationnelles. Cela autorise également leur efficacité et efficience.

Assurer la cybersécurité d'un pays, c'est aussi appréhender les enjeux et les impacts de l'évolution numérique dans le secteur militaire, de la défense et de l'armée. Le cyberespace est désormais considéré comme le cinquième champ de bataille. Il est un terrain d'opérations militaires au même titre que la terre, la mer, l'air et l'espace.

Le monde civil et le monde militaire sont appelés à maîtriser les cyber risques, que cela soit à des fins économiques, de lutte contre la cybercriminalité, soit dans un but de sécurité et de défense nationales. La transversalité d'Internet, la prégnance des technologies informatiques, les compétences nécessaires à la maîtrise des infrastructures numériques et à leur sécurité, les besoins d'efficacité et de synergie, contribuent à faire émerger des approches globales et systémiques que reflète la notion de continuum de cybersécurité et de cyberdéfense.

La dimension internationale d'Internet et du cybercrime, le monde globalisé et interconnecté dans lequel nous vivons, constituent également de nouveaux défis à la maîtrise des cyber risques, qui

deviennent de plus en plus complexes et globaux et dont les effets en cascade peuvent avoir des impacts immédiats ou différés, parfois loin de leur origine géographique. Toutes ces raisons accroissent la nécessité de collaboration et de coopération aux niveaux national et international.

Maîtriser les cyber risques ne se limite pas à la mise en place de « rustines technologiques » pour pallier les vulnérabilités des produits conçus sans prise en compte des besoins de sécurité et de protection des données. En effet, il s'agit d'être en mesure de maîtriser toutes les dimensions du risque que fait porter l'usage extensif des technologies de l'information et de la communication sur la société. Lutter efficacement contre la cybercriminalité passe par une approche préventive qui consiste à rendre le cyberespace moins favorable à l'expression de la criminalité et à réduire les opportunités criminelles. Il faut élever le seuil de difficulté de réalisation des cyberattaques (augmenter les coûts en termes de compétences et de ressources pour le malveillant et diminuer les profits attendus) et accroître les risques pris par les criminels d'être identifiés, localisés et poursuivis.

Il est dès lors nécessaire et urgent de contribuer à :

- la réduction du nombre de vulnérabilités techniques, organisationnelles, juridiques et humaines exploitées à des fins malveillantes ;
- la robustesse et à la résilience des infrastructures informatiques par des mesures de sécurité technologiques, procédurales et managériales cohérentes et complémentaires ;
- développer une réelle capacité d'adaptation des moyens de cybersécurité et de cyberdéfense pour répondre à une situation en constante évolution ;
- disposer de moyens pour gérer les crises « cyber ».

Cela signifie également que ces actions doivent s'inscrire dans une volonté politique forte et un engagement des États à faire de la lutte contre la cybercriminalité et du renforcement des capacités de cybersécurité et de cyberdéfense une priorité.

C'est en agissant sur de multiples facteurs dans les domaines politique, socio-économique, juridique et technique que des éléments de réponse peuvent être apportés aux besoins de sécurité et de respect des droits fondamentaux des personnes, notamment le respect de la vie privée, de l'intimité numérique et de la liberté d'expression. Les mesures de sécurité et de défense adoptées doivent être appropriées et proportionnées aux menaces et aux risques effectifs. Mobiliser, fédérer et engager les différents acteurs privés et de la société civile autour de la lutte contre la cybercriminalité et de la construction d'un écosystème numérique de confiance est tout aussi important que de développer des capacités humaines compétentes ainsi que de mettre en place des actions de sensibilisation et de formation de tous les acteurs.

Introduction

Les progrès socio-économiques et techniques ont mis l'informatique à la portée de toutes les nations et de la grande majorité des citoyens. Les secteurs privé et public, comme les individus ont intégré les technologies de l'information et de la communication dans leurs quotidiens. Bien que disponible de manière inégalitaire, Internet est présent dans presque tous les pays du monde. La téléphonie mobile et les services offerts sur les smartphones occupent progressivement la première place dans les moyens de communication et d'accès à l'information.

Qu'il s'agisse des finances publiques, des ressources humaines, de la communication, tous les gouvernements disposent à l'heure actuelle de systèmes d'information de taille et de complexité variées. D'une manière générale, le fonctionnement et la modernisation de l'État, l'administration publique s'appuient sur des infrastructures informatiques et la dématérialisation des services pour une plus grande efficacité et l'amélioration des services rendus aux usagers. Même si le « gouvernement électronique » est loin d'être une réalité pour tous les pays, presque partout dans le monde, le déploiement du gouvernement électronique constitue l'une des stratégies qu'utilisent les pays pour mieux faire face aux défis économiques du vingt et unième siècle.

Nombre des systèmes d'information ainsi déployés constituent des infrastructures critiques pour les pays : leur incapacité à être opérationnels du fait d'incidents de sécurité non maîtrisés pourrait porter atteinte au fonctionnement de l'État, à la sécurité nationale, au bien-être économique et social des personnes. L'actualité ne cesse de démontrer que la probabilité de dysfonctionnement ou d'indisponibilité est loin d'être négligeable, que cela soit dû à une erreur, un accident ou que cela relève de la malveillance.

C'est de la responsabilité de chacun, d'agir de sorte à réduire le nombre et surtout les impacts des incidents de sécurité. En effet, les intrusions dans des systèmes informatiques, les atteintes à la confidentialité, à l'intégrité ou à la disponibilité des systèmes, le vol de données, la prise de contrôle à distance ou le sabotage engendrent des pertes directes ou indirectes pour les entités qui en sont victimes et qui portent atteinte à leur pérennité et compétitivi-

té. De plus, le grand degré d'interconnexion des systèmes d'information dans un monde globalisé et interdépendant fait qu'un problème sur une entité peut entraîner des effets en cascades sur d'autres (notion de risque systémique) aux impacts directs ou indirects et des effets immédiats ou sur le plus long terme.

« Le défi de la cybersécurité est mondial, car le phénomène touche tous les pays du globe, mais comporte une dimension qui met en cause les frontières terrestres et projette les populations dans une société de l'information mondialisée. Le cyberespace est par définition virtuel ; il s'agit pour les États de faire valoir les frontières et la sécurité dans cet espace virtuel mondialisé, et d'assurer aux citoyens, aux entreprises et aux institutions un État de droit dans le cyberespace ».

Note conceptuelle « Conférence internationale sur le renforcement de la cybersécurité et de la cyberdéfense dans l'espace francophone ». OIF. Abidjan, Côte d'Ivoire ; 8 — 10 février 2016. : francophonie.org/IMG/pdf/note_conceptuelle_conference_cybersecurite_abidjan_2016.pdf

NÉCESSITÉ D'ACTION

Le numérique peut contribuer au développement des services et être un véritable levier économique. Il permet entre autres de faciliter les mises en relation, l'offre et la demande, l'accès à l'information et à l'éducation. Il peut également avoir un rôle dans des mesures d'aménagement du territoire ou de gestion des ressources. Les possibilités offertes par l'identité numérique sont nombreuses dans tous les domaines d'activité et en particulier dans le domaine de la santé, du commerce électronique et des paiements et transactions financières dématérialisés, de la lutte contre des fraudes, du recensement de la population ou encore du contrôle social ou des populations pour ne donner que quelques exemples*.

Chaque évolution est porteuse d'opportunités, mais aussi de risques que cela soit pour les individus, les organisations publiques et privées ou l'état et la société.

PRINCIPAUX IMPACTS DES CYBERRISQUES SUR LES PERSONNES

Internet permet de communiquer avec potentiellement tout le monde, et donc n'importe qui. Il est difficile, voire impossible de vérifier qui se cache derrière un écran, à distance ou derrière une identité virtuelle, une fausse identité ou un pseudonyme. Il n'existe pas de mécanisme « de sécurité » qui permet de garantir la bonne foi des internautes encore moins des robots logiciels qui alimentent les plateformes de communication.

Tous les acteurs de l'Internet peuvent agir de manière bienfaisante et/ou malveillante, loyale et/ou déloyale.

C'est à l'internaute de rester vigilant et de décider par lui-même si ce qu'il voit sur son écran est vrai ou faux, s'il s'agit d'une publicité ou encore une tentative d'escroquerie et s'il peut accorder sa confiance ou non, s'il souhaite interagir avec l'entité avec laquelle il est en contact.

*Par ailleurs, le numérique est le plus souvent le support à l'identité des individus de par l'usage de documents d'identité biométrique (carte nationale d'identité, passeport biométrique, permis de conduire).

De plus, un sentiment de « confiance et de proximité » que rien ne permet de justifier, ni de garantir de manière fiable et durable est le plus souvent entretenu par les fournisseurs de services de socialisation. L'impression d'être « entre amis » génère un faux sentiment de sécurité qui peut avoir des répercussions désastreuses sur la vie des personnes. La liste 1 présente les risques auxquels peuvent être exposés et confrontés les internautes.

Liste 1 : exemples de risques dont peut être victime un individu.

- Harcèlement, intimidation, chantage, incivilités, etc.
- Diffamation, mise à mal de la réputation.
- Exposition à des contenus malveillants, offensifs ou non désirés (virus, spam, pornographie dure, scène de violence, incitation à la haine raciale et à la xénophobie, propagande, etc.), à des publicités intrusives, canulars, escroqueries, chantages, fraudes ou abus en tout genre.
- Objet de surveillance, de traçabilité, de profilage excessif, d'écoutes environnementales (atteinte à la vie privée et à l'intimité numérique, espionnage).
- Vol de données : données personnelles, informations confidentielles, propriété intellectuelle, etc.)
- Vol d'équipements (ordinateur, clé USB, CD-ROM, etc.)
- Destruction de valeurs.
- Usurpation d'identité.
- Désinformation, manipulation d'opinion, influence.
- Usage détourné des capacités informatiques.
- Prise de contrôle des systèmes par des entités tierces.

PRINCIPAUX IMPACTS DES CYBERRISQUES SUR LES ORGANISATIONS

Parmi les risques spécifiques aux institutions, qu'elles soient privées ou publiques, retenons notamment les risques présentés dans la liste 2.

Liste 2 : synthèse des principaux problèmes d'origine cybercriminelle auxquels doivent faire face les organisations.

- Espionnage industriel et économique (vol/perte de secrets des affaires, de valeurs immatérielles, de savoir-faire, etc.)
- Attaques concurrentielles (vol de fichiers clients, de prix, de fournisseurs, de plan de fusion-acquisition, etc.)
- Atteintes à la propriété intellectuelle, au droit des marques, etc.
- Attaques sémantiques (rumeurs, fausses informations, manipulation d'information, désinformation, etc.)
- Atteintes à l'image, à la réputation, à la fiabilité, etc.
- Incapacité à produire, à fonctionner (dysfonctionnements, indisponibilité des ser-

vices, perte de qualité, altération des processus décisionnels, etc.)
- Falsification, défiguration de sites web.
- Infection des ressources informatiques, détournement des capacités informatiques.
- Prise de contrôle des ressources informatiques à des fins de chantages.
- Criminalité financière et économique.

PRINCIPAUX IMPACTS DES CYBERRISQUES POUR L'ÉTAT

Plus les États sont développés, plus leur capacité militaire et leur pouvoir économique sont dépendants des technologies du numérique. De ce fait, ils peuvent être fragilisés, car ils sont plus vulnérables aux attaques informatiques majeures. Le tableau 1 présente une synthèse des principaux types de risques et d'impacts pour un pays.

Tableau 1 — Récapitulatif des impacts des principales cyberattaques pour un État.

Cyberattaques sur :	Impacts potentiels sur :
Des systèmes informatiques contrôlant les infrastructures critiques	Population Économie Sécurité nationale Sûreté publique Centres d'alerte et de secours Fonctionnement du gouvernement, l'administration Chaînes d'approvisionnement
Des systèmes informatiques relatifs à la prise de décisions dans le secteur de la défense militaire et sur des systèmes d'armement (contrôle de missiles, drones, aviation militaire, équipement du soldat…)	Centres névralgiques nécessaires au commandement militaire et à l'opérativité de l'armée Altération des processus de prise de décisions La disponibilité et la qualité des informations nécessaires à la prise de décision pertinente Le commandement stratégique et opérationnel Le champ de bataille L'art de faire la paix et la guerre La manière de gérer les conflits, de les prévenir, de les traiter Invalidation des défenses de l'adversaire
L'information (manipulation de) constituant des stratégies d'influence et de guerre psychologique	Le moral des troupes, de l'opinion publique, les dirigeants économiques et politiques La manipulation des foules, capacité à soulever des manifestations hostiles contre l'État (activisme, terrorisme, rassemblement…) Déstabilisation des services de renseignement Diplomatie internationale

Aux risques précédemment présentés, il convient d'y associer ceux liés à l'écologie du numérique, notamment pour ce qui concerne les risques induits par la consommation énergétique nécessaire aux fonctions des ordinateurs, équipements électroniques, téléphones,

réseaux de télécommunication, fermes de serveurs, satellites de communication ou encore par exemple, aux systèmes d'information de support, aux infrastructures informatique et télécom.

Au risque énergétique majeur, s'ajoute celui lié aux traitements des déchets électroniques, à la pollution, au réchauffement climatique (dégagement de chaleur et besoin de refroidissement des ordinateurs et fermes de serveurs), à l'épuisement des matériaux constitutifs des équipements (silice, cuivre…), aux conséquences environnementales d'incidents provoqués par des cyberattaques sur des systèmes contrôlant des stations d'épuration, la production et la distribution de produits toxiques ou encore sur des alarmes incendie, par exemple.

Les risques « cyber » s'inscrivent dans une problématique plus large des risques liés à la dépendance des infrastructures numériques et à des fournisseurs d'infrastructures matérielles et logicielles, de capacités de traitement, de télécommunication, de stockage, de services (informatique en nuage – cloud computing, big data, téléphonie, Internet, etc.)

Certains fournisseurs sont devenus des géants incontournables de l'Internet ou de la téléphonie mobile, et sont de véritables empires à la volonté hégémonique affichée.

La montée en puissance de certains groupes mondialisés, induit de nouveaux risques notamment liés et à leurs capacités à pouvoir réaliser des actions d'intelligence économique, de surveillance, d'espionnage ou encore de « filtrage » des échanges et cela à l'échelle mondiale. Par ailleurs, au niveau individuel, certaines personnes développent des comportements et des habitudes de consommation du numérique (médias sociaux, divertissements, jeu d'argent, sexe, etc.) qui peuvent relever de phénomène d'addiction les empêchant d'être présents au monde et responsable, ou encore de s'alimenter, de dormir suffisamment, de travailler, d'établir des liens réels avec des personnes physiques bien vivantes, dans leur environnement physique réel (tableau 2).

Tableau 2 — Risque de dépendance numérique pour la société.

Risque de dépendance pour :	Principales questions soulevées :
La société et l'État	Avec la dépendance à des acteurs économiques tiers, généralement étrangers, comment satisfaire le besoin de souveraineté nationale ? Comment assurer un développement durable et maîtrisé de l'économie numérique ?
L'individu	Comment éviter la consommation addictive du numérique ? Comment éviter les comportements addictifs pouvant porter atteinte à l'intégrité physique et morale des personnes ? Comment protéger les personnes contre leur volonté ?

Par ailleurs, c'est généralement sous couvert d'aide au développement que les acteurs puissants de l'Internet étendent leur pouvoir et assujettissent de nouveaux consommateurs en proposant des services gratuits et/ou en contribuant aux déploiements d'infrastructures de télécommunication. Ce type de démarche pose des problèmes de dépendance et de perte de

souveraineté aux pays qui ne peuvent être autonomes en matière de numérique, qui dès lors, pourraient devenir captifs de fournisseurs étrangers dont ils subiraient la colonisation numérique. Il est vrai que cette question de dépendance à des équipementiers ou des fournisseurs de services étrangers est un problème crucial auquel doivent faire face de nombreux pays. Cette prise de conscience est pour beaucoup, consécutive aux révélations de cyberespionnage et de surveillance de masse, rendues publiques par un ex-agent de l'agence de sécurité nationale (NSA — National Security Agency) des États-Unis d'Amérique en 2013*.

Face à un ensemble de menaces complexes et multiformes potentiellement perturbantes, voire destructrices, la passivité des gouvernants dans le domaine cyber ne peut être de mise et la possibilité d'une autorégulation est illusoire, car elle ne bénéficierait qu'aux acteurs les plus puissants. La sécurité joue un rôle essentiel dans le développement de l'économie basée sur le numérique. Pour garantir leur sécurité, soutenir leur économie, contribuer à leur souveraineté, tous les pays se doivent de posséder des stratégies liées à l'économie numérique et de renforcer leur posture de cybersécurité et de cyberdéfense. Désormais, ce sont des objectifs qui doivent figurer en bonne position dans les priorités de l'élaboration des politiques gouvernementales.

PLAN D'ACTION

Partant du fait qu'il est difficile d'intervenir sur un phénomène qui reste malgré tout récent et qui continue de se développer rapidement et qui par conséquent n'est pas forcément bien connu, il est important pour chaque pays de pouvoir établir un état des lieux de sa situation en matière de cybersécurité et de cyberdéfense afin d'être en mesure d'identifier et de dégager les moyens nécessaires à sa transformation numérique. Cela peut être envisagé sous la forme de la réalisation du diagnostic de la situation nationale, d'une analyse des vulnérabilités, des menaces et des risques afin de piloter, développer, mettre en œuvre, optimiser les plans d'action stratégique et opérationnelle permettant la maîtrise des cyberrisques auxquels chaque pays est désormais confronté.

La mise en œuvre des actions qui émergeront des recommandations nécessitera une batterie de ressources financières et organisationnelles, ainsi que des mesures de coopération et de coordination au plan national, régional et international. Toutefois, la ressource critique et centrale au succès du développement numérique demeure toujours l'humain et ses compétences. Il est donc également primordial d'intégrer au plus tôt dans toute démarche de transformation numérique de la société un plan de développement des capacités humaines, basé sur la sensibilisation de toute la population (du plus jeune au plus âgé), et sur la formation et la recherche, que cela soit dans des domaines technique, juridique, économique, politique, ou social.

*Edward Snowden - fr.wikipedia.org/wiki/Edward_Snowden

Investir dans l'éducation et la recherche sont les leviers du développement de l'économie numérique, permettant l'innovation, l'émergence de nouveaux services, métiers et formes de travail. De plus, cela contribuera, à court et à long terme, à la disponibilité des capacités et compétences nécessaires à la société de l'information et à la maîtrise des cyberrisques.

Les actions humaines s'exprimant au mieux lorsqu'elles s'inscrivent dans un cadre bien organisé, dans une vision partagée et réglementée, il est nécessaire de créer les cadres législatifs et organisationnels adéquats pour assurer la cybersécurité et la cyberdéfense. Cette dimension de la mise en place de cadres adéquats ne doit pas oblitérer le besoin de réponse immédiate aux situations d'urgence. C'est au regard de cet ensemble de considérations que ce guide propose aux dirigeants de :

- conduire le diagnostic de l'état de cybersécurité et de cyberdéfense dans leur écosystème ;
- identifier leurs infrastructures critiques et de garder un œil vigilant sur les tous les opérateurs d'importance vitale ;
- mettre en œuvre une structure de réponse d'urgence aux incidents de sécurité de l'information ;
- définir des mécanismes appropriés de protection des données à caractère personnel ;
- définir des mécanismes appropriés de protection des enfants, de la jeunesse, des plus faibles, dans le cyberespace ;
- développer le capital humain pour assurer la cybersécurité et la cyberdéfense ;
- déployer les structures organisationnelles de la cybersécurité et de la cyberdéfense ;
- développer les mesures législatives devant réguler la cybersécurité et la cyberdéfense ;
- assurer coopération et coordination nationale, régionale et internationale dans le cadre de la cybersécurité et de la cyberdéfense ;
- élaborer une stratégie nationale de cybersécurité et cyberdéfense et d'en assurer la mise en œuvre effective, le contrôle, l'évaluation et l'optimisation.

ANALYSE DES RISQUES ET MESURES DE SÉCURITÉ

PRINCIPES FONDAMENTAUX

Il existe des points communs et des similarités dans les économies modernes en termes de leurs degrés de mise en œuvre du numérique, mais les spécificités de chaque pays demeurent. Il est important, pour un dirigeant d'avoir à une très bonne connaissance de son écosystème numérique (figure 1) et des risques afférents.

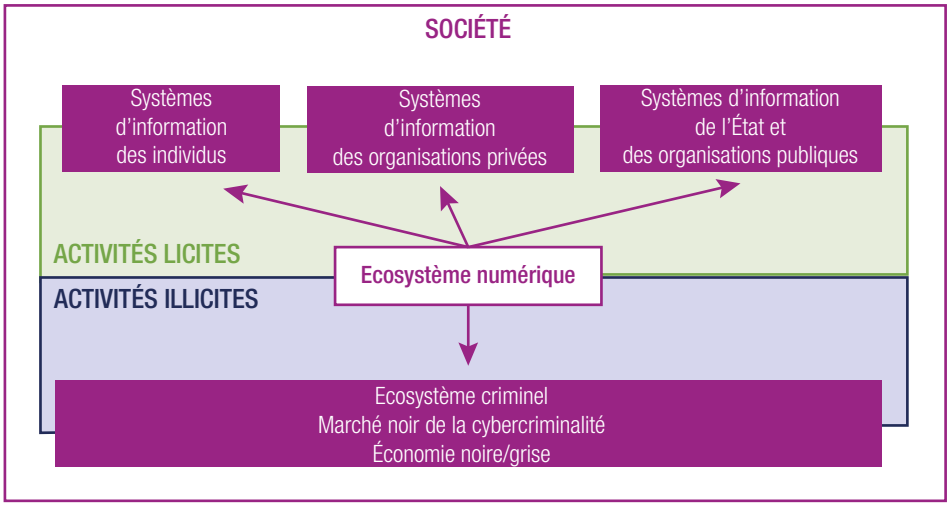


Figure 1 — L'écosystème numérique (adaptée du livre *Cyberpower, crime, conflict & security in cyberspace*, S. Ghernaouti, EPFL Press, 2013)

Cette connaissance inclut des éléments tels que les utilisations effectives des technologies de l'information et de la communication du pays, les infrastructures informatiques et des télécommunications, le cadre organisationnel, le cadre législatif, les acteurs et fournisseurs, la disponibilité des compétences humaines, les impacts de l'économie numérique (impacts politique, économique, social et financier), la création d'emplois et les mutations en cours, etc.

Tous ces éléments devront concourir à une appréciation rigoureuse non seulement des risques encourus, des besoins de sécurité, mais aussi des moyens à disposition et des interdépendances afin de permettre une identification des leviers d'action et des mesures de cybersécurité à mettre en œuvre. Cela relève d'une approche de type « diagnostic ». En effet, un diagnostic permet d'apporter des réponses à des questions essentielles telles qu'entre autres :

- quelles sont les valeurs à protéger ?
- quels sont les actifs informationnels ?
- quelles sont les infrastructures critiques ?
- quelles sont les vulnérabilités techniques, organisationnelles, juridiques, humaines ?
- quelles menaces pourraient exploiter les vulnérabilités ?
- quels sont les impacts des cyberrisques sur les institutions publiques, le fonctionnement de l'État, les infrastructures critiques, les entreprises et la population ?
- quels sont les besoins stratégiques et opérationnels de la cybersécurité ?
- quels sont les défis actuels et envisageables en matière de maîtrise des cyberrisques et de cybersécurité ?
- quelles sont les parties prenantes de la stratégie nationale de cybersécurité, aux niveaux local, régional et international ?
- quels sont les partenariats public — privé possibles ? Comment les construire afin que les risques et profits soient partagés de manière équilibrée ?
- quelles sont les ressources disponibles et potentielles ?
- quels les niveaux de sécurité et de résilience souhaités ?
- etc.

Un risque est un danger éventuel plus ou moins prévisible. Il se mesure à la probabilité qu'il se produise et aux impacts et dommages consécutifs à sa réalisation.

Le risque « Cyber » est lié à l'usage extensif des technologies de l'information et des communications. Il s'agit d'un risque structurel, omniprésent et permanent dont l'origine peut être de nature criminelle, liée à des actions offensives, à des erreurs involontaires ou encore résultantes d'accidents naturels (figure 2). Connaître, identifier, évaluer les cyberriques auxquels les institutions et les individus sont exposés permet de concevoir et de mettre en place des mesures adéquates de sécurité pour les maîtriser et minimiser leurs impacts négatifs.

Maîtriser un risque revient à mettre sous contrôle les facteurs qui le composent. En effet, un système est à risque si des vulnérabilités et des menaces lui sont associées et que la réalisation de ces menaces (dangers potentiels pouvant l'affecter) induisent des dégâts. On parle alors d'impacts négatifs ayant des conséquences sur le système (son état, son fonctionnement) ou affectant son environnement ou son propriétaire.

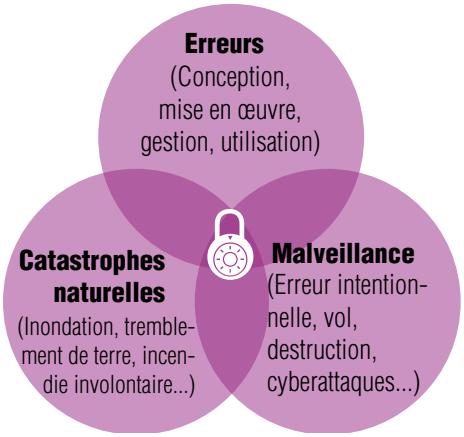


Figure 2 — Origines des incidents pouvant conduire à des problèmes de cybersécurité

DU DIAGNOSTIC AUX MESURES DE SÉCURITÉ

Un diagnostic permet de procéder à une analyse des risques, de les identifier, évaluer, répertorier, par le biais des événements redoutés et des scénarios de menaces, en prenant en compte l'environnement interne, externe, les vulnérabilités connues, les différentes contraintes actuelles et potentielles. L'analyse de risques permet d'identifier les mesures stratégiques, organisationnelles, procédurales et techniques nécessaires à l'atteinte des objectifs de sécurité (figure 3). Il est important de développer et de mettre en œuvre une méthode d'analyse des risques basée sur une taxonomie commune, une terminologie comprise afin que chaque partie prenante possède le même référentiel de vocabulaire et puissent développer une vision commune et harmonisée des besoins de sécurité et des mesures pour y pallier*.

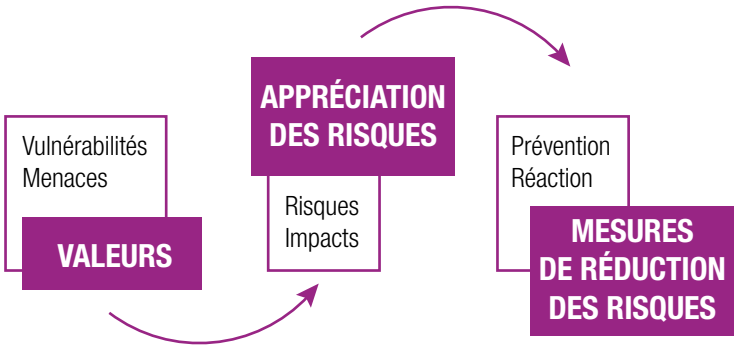


Figure 3 — Démarche d'analyse des risques : comprendre ses valeurs pour mieux les protéger

*Pour information, l'Agence Nationale française de la Sécurité des Systèmes d'Information (ANSSI) met à disposition la méthode d'analyse de risques EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) qui est accessible sur son site : ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/. Il existe plusieurs autres méthodes ou normes dont ISAMM en Belgique, Mehari et ISO 17799.

Un diagnostic peut se visualiser sous la forme de tableaux de matrice de risques (Figure 4). Cela permet de visualiser pour chaque type de risque, sa probabilité d'occurence (très fréquent, fréquent, rare, exceptionnel) et son niveau d'impact (très grave, grave, moyennement grave, faible).

Pour chaque contexte faisant l'objet d'un diagnostic, des critères d'évaluation peuvent être spécifiquement définis et l'échelle de probabilité ou d'impacts affinés en fonction du degré de finesse souhaité de l'analyse. Il est souvent souhaitable de quantifier les niveaux pour mieux les évaluer et suivre leur évolution. C'est généralement par rapport à une perte financière que les impacts sont évalués, celle-ci est spécifique à l'institution concernée. Par exemple, la perte de 10 000 euros pourrait être considérée comme mineure pour une banque alors que l'impact pour une PME serait sans doute grave.

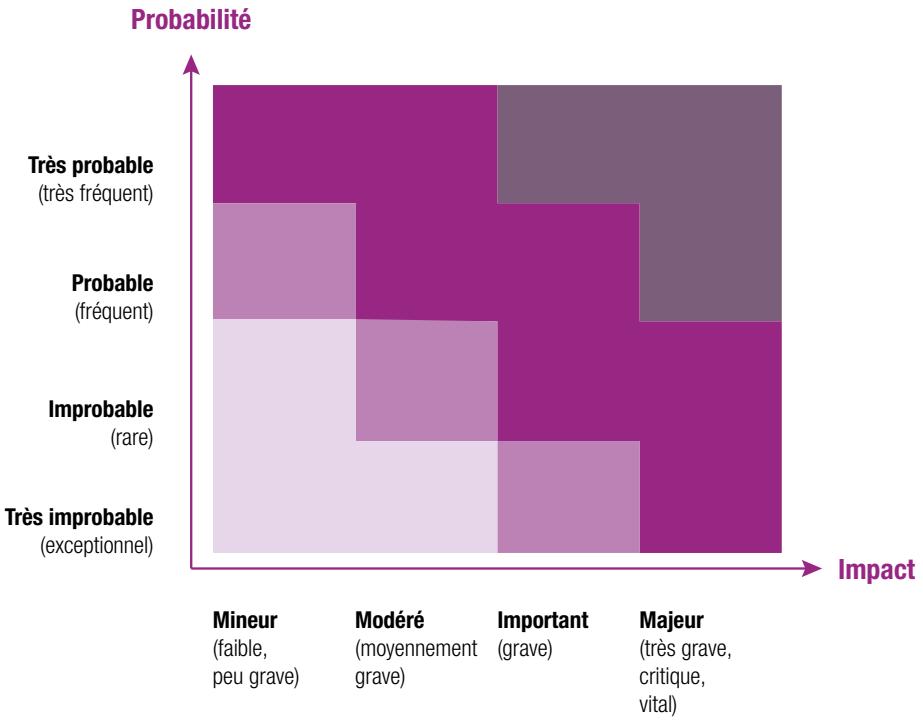


Figure 4 — Exemple de matrice des risques

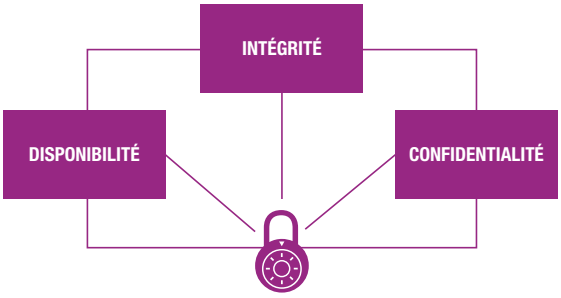


Figure 5 — Critères fondamentaux de la sécurité informatique

De manière générale, un cyberrisque se matérialise par la réalisation d'une cyberattaque qui affecte tout ou partie des critères de sécurité d'un système informatique, à savoir : la disponibilité, l'intégrité et la confidentialité (figure 5).

La disponibilité d'une ressource qualifie le fait qu'elle peut être utilisée pour rendre le service pour lequel elle a été conçue. Certaines attaques informatiques consistent à rendre indisponibles des ressources, portant ainsi préjudice non seulement aux utilisateurs, mais aussi aux propriétaires et exploitants de la ressource.

C'est le cas par exemple d'attaque en déni de service d'un système, ou de son blocage par un programme malveillant (rançongiciel) qui le prend en otage en le chiffrant et demande au propriétaire une rançon pour le rendre à nouveau disponible.

L'intégrité d'une ressource est relative au fait qu'elle n'a pas été altérée ou détruite de manière non intentionnelle. Par exemple, certains actes malveillants consistent à modifier ou à falsifier des informations afin d'infléchir une prise de décision particulière (modification du cours de la bourse entraînant l'achat ou la vente d'actions, par exemple).

La confidentialité est le maintien du secret de l'information. En tant que critère de sécurité, la confidentialité est la protection des données contre une divulgation non — autorisée. La confidentialité des données peut être mise à mal par des écoutes passives (surveillance, espionnage. écoute) ou par le vol de données qui consiste en réalité en leur copie, ce qui est parfois difficile à se rendre compte puisque les données ne sont pas volées à proprement parler.

L'objet des mesures de sécurité est de :
• limiter l'intensité et l'ampleur des dégâts induits par des risques ;
• se prémunir contre les menaces potentielles par des mesures de protection et de prévention appropriées ;
• pouvoir réagir aux incidents par des mesures de réaction, notamment par des mesures de gestion de crise, de gestion de la continuité des activités, de reprise des activités ou encore des mesures de poursuite pénale, si nécessaire.

À partir de ces critères de base des exigences de sécurité additionnelles peuvent être identifiées comme par exemple, l'authenticité, la véracité, l'imputabilité, la non-répudiation ou encore la vérificabilité (auditabilité).

MESURES STRATÉGIQUES ET OPÉRATIONNELLES DE SÉCURITÉ

Pour satisfaire les critères fondamentaux de la sécurité, il est nécessaire de mettre en place des mesures de sécurité appropriées, par exemple des mesures de contrôle d'accès, d'identification, d'authentification, de non-répudiation, de surveillance, d'enregistrement, de cloisonnement d'environnement, de surveillance, de chiffrement, etc.

La figure 6 propose une typologie des principales mesures de sécurité possibles pour renforcer la sécurité des infrastructures numériques.

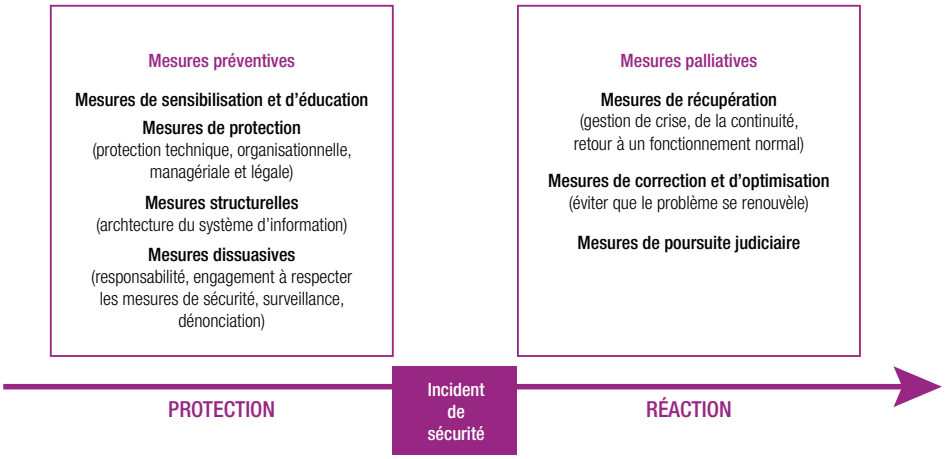


Figure 6 — Typologie des principales mesures de sécurité d'un système d'information

Un modèle de maturité permet de situer sur un graphique, le niveau de sécurité actuel, de visualiser le niveau souhaité à atteindre et de suivre son évolution dans le temps. Un modèle de maturité peut être considéré comme un outil de pilotage et de suivi de la sécurité d'un système afin d'en apprécier son degré de maturité au regard d'exigences de sécurité. Il peut s'apparenter à un véritable tableau de bord alimenté automatiquement qui permet de rapporter et de contrôler les actions de sécurité en vue de leur amélioration et optimisation.

Pour répondre aux cybermenaces, la figure 7 résume la démarche de cybersécurité à gérer et à mettre en œuvre au sein des institutions publiques ou privées, afin qu'elles puissent mieux maîtriser leurs cyberrisques. Toutes les entreprises indifféremment de leur taille ou de

Modèle de maturité de la sécurité d'un système
Un modèle de maturité est une sorte d'échelle de mesure, de thermomètre de l'état de sécurité d'un système ou d'environnement, servant pour l'essentiel à indiquer ou à mesurer à quel niveau de sécurité il se situe, en fonction de certains critères ou métriques préalablement établis, afin de pouvoir évaluer sa qualité, son niveau de conformité réglementaire, l'améliorer, suivre son évolution ou encore par exemple, le comparer à d'autres.

leur nombre d'employés doivent être sensibilisées aux besoins de cybersécurité et adopter à minima une certaine hygiène informatique, un comportement et un usage de l'informatique cohérents au regard des risques pour ne pas contribuer à exposer leurs données et infrastructures informatiques et à les mettre en danger.

La sécurité informatique ne doit pas être considérée comme un frein aux affaires, mais comme un levier permettant de les réaliser. Elle contribue à ce qu'une organisation soit compétitive et pérenne.

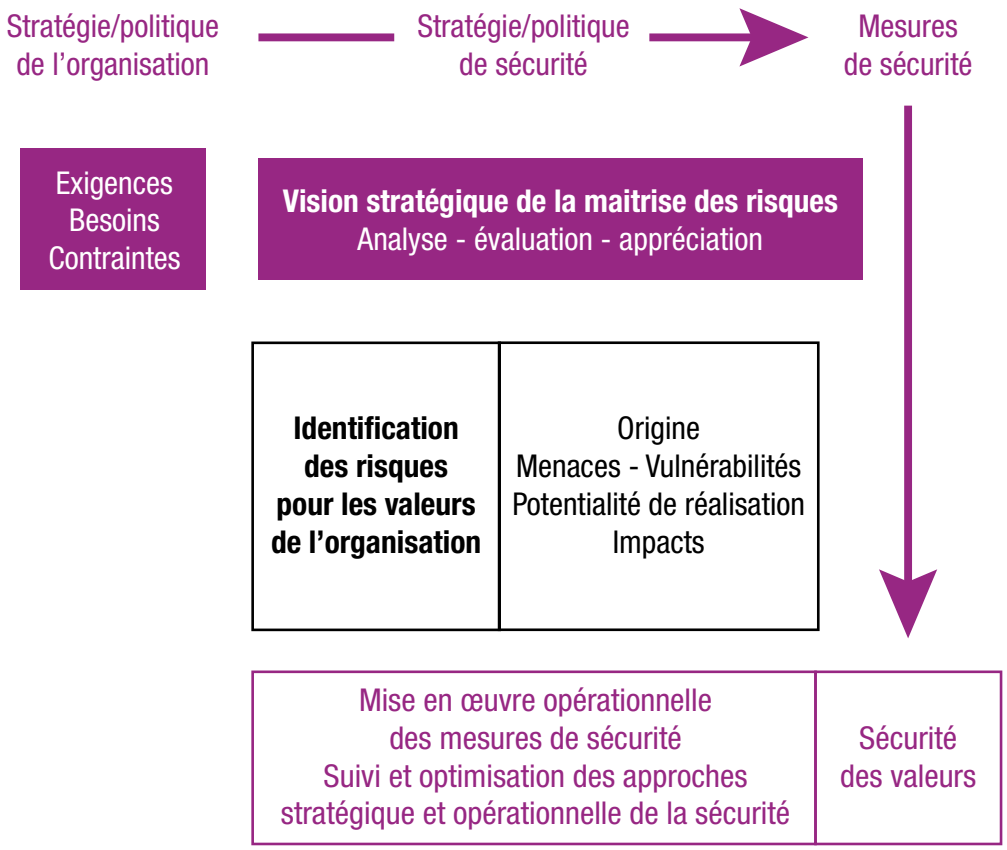


Figure 7 — Complémentarité et cohérence des approches de gestion des risques et de gestion de la sécurité

Chaque environnement à protéger est spécifique et requiert une démarche de sécurité appropriée. Par ailleurs, il est possible d'externaliser tout ou partie de ses services informatiques chez des fournisseurs externes (notion d'informatique en nuage – *cloud computing*) et de ce fait d'externaliser aussi sa sécurité.

Une relation de confiance doit alors pouvoir s'établir avec le prestataire de service à qui l'entreprise confie son outil de travail et ses ressources informationnelles. La confiance peut être bâtie sur la base d'un accord contractuel qui spécifie les rôles et responsabilités de chacune des parties et sur des mesures de vérification du respect des engagements et des conséquences d'un défaut de sécurité du prestataire, que cela soit par erreur, négligence ou incompétence ou encore suite à une intrusion et attaque sur les serveurs des prestataires.

Un des problèmes posés par l'usage des solutions clés en main d'externalisation et d'informatique en nuage est celui lié à l'incapacité de savoir où sont stockées physiquement les données, comment elles sont protégées, quels sont les acteurs qui y accèdent vraiment et pour quoi faire, quel est le droit applicable, comment faire recours en cas de problème, etc. De plus, l'individu comme l'organisation sont totalement tributaires de la disponibilité des réseaux de télécommunication pour accéder à leurs propres données et dépendants du prestataire à qui ils ont délégué leur capital numérique.

Avant d'externaliser tout ou partie de son informatique ou de sa sécurité et de devenir dépendant d'un fournisseur, il est nécessaire de se poser la question de savoir si les économies à court terme, induites par une telle sous-traitance, sont justifiées en regard de la perte de la maîtrise des technologies, de la sécurité, des savoir-faire et du risque de détournement d'information ou d'exploitation abusive des données.

Par ailleurs, il est impossible pour une entreprise de pouvoir effectuer des audits de son système informatique lorsque celui-ci est hébergé sur des infrastructures tierces et potentiellement dans des pays étrangers. Par exemple, une entreprise pourrait avoir des problèmes liés au fait qu'elle ne soit pas en règle avec la conformité juridique et réglementaire dans son propre pays alors qu'elle ne maîtrise pas directement le traitement et l'hébergement de ses données.

Pour une organisation, les principes généraux d'une démarche de gouvernance de la cybersécurité peuvent s'articuler autour des mots clés suivants* :

1. Responsabilité — Chaque instance assurant la gouvernance doit être responsable de la tâche qui lui incombe.
2. Proportionnalité — Les investissements doivent être proportionnels au risque informationnel encouru par l'entreprise.
3. Conscience — Les instances directrices sont conscientes du rôle et de l'importance des actifs informationnels de l'entreprise et, par conséquent, du rôle et des besoins de sécurité.
4. Conformité — Les stratégies et les mesures sécuritaires doivent être conçues, mises en place et gérées en conformité avec les exigences légales et réglementaires.
5. Efficacité et efficience – Les mesures répondent aux exigences de sécurité de manière optimale et satisfaisante y compris sur le plan financier.

*Source : Solange Ghernaouti, *Cybersécurité : Sécuité informatique et réseaux*. Dunod 5e édition, 2016.

6. Inclusion — Les exigences de toutes les parties intéressées par la démarche (parties prenantes) doivent être prises en considération.
7. Transparence — Le devoir d'informer les parties intéressées sur l'état courant de la sécurité incombe aux instances directrices.
8. Éthique — La démarche de sécurité doit respecter les valeurs d'éthique communément admises, en particulier les droits humains fondamentaux.
9. Équité — Les instances directrices mettent en œuvre les solutions sécuritaires basées sur la perception et les règles démocratiques perçues comme telles dans l'environnement où l'entreprise agit.
10. Suivi — Des évaluations doivent être réalisées périodiquement afin de s'assurer de la pertinence des réponses apportées au regard de l'évolution des risques.
11. Gestion du risque — Les instances directrices s'assurent que le processus d'appréciation des risques se fait d'une manière continue et formalisée et est en cohérence avec la gestion de la sécurité.
12. Culture de la sécurité — Une culture de la sécurité doit être développée afin que tous les acteurs développent des comportements cohérents et soient acteurs de la sécurité.

ASPECTS JURIDIQUES

CADRE LÉGISLATIF

Dans certains pays, le cadre législatif actuel offre peu de disposition permettant d'encadrer les activités dématérialisées de l'économie numérique et par extension pour encadrer celles liées à la cybersécurité et à la cyberdéfense. Dans les cas où des textes légaux existent, ils peuvent vite devenir obsolètes s'ils sont liés à des techniques particulières ou à des contextes d'usages spécifiques, dans la mesure ou l'environnement du numérique évolue rapidement et en permanence. De nouveaux services, intermédiaires techniques, applications, comportements ou encore de nouvelles formes de malveillance émergent de l'écosystème numérique en fonction de son évolution dynamique. C'est pourquoi la conception des textes de loi doit être suffisamment générique pour être indépendante des technologies et pourra s'attacher à la protection des consommateurs, à la protection des données à caractère personnel ou encore à la répression du cybercrime. De plus, le cadre juridique a également pour objet de d'encadrer les actions du gouvernement et des acteurs privés dans le domaine de la cybersécurité et de la cyberdéfense.

Il s'agit d'une part, d'autoriser légalement et de cadrer les cyber actions intervenant dans des stratégies civile et militaire de la lutte contre la cybercriminalité, et d'autre part, d'encadrer les activités de cybersécurité et de cyberdéfense. Cela permet de fixer le domaine de compétence des acteurs et de donner les moyens aux protagonistes de réaliser leur mission, mais aussi à la société de contrôler la légalité des actions (informatique offensive, défensive, respect des droits fondamentaux des individus, etc.). Cette action est particulièrement importante, lorsque cela concerne les pratiques de renseignement, de perquisition à distance dans des systèmes d'information, l'usage de programmes pour surveiller, infiltrer, prendre le contrôle à distance, etc.

En fait, une référence internationale en matière de cadre légal concernant la lutte contre la cybercriminalité existe depuis 2001. Bien qu'il s'agisse d'un instrument régional, la Convention européenne sur la cybercriminalité du Conseil de l'Europe* pose les bases nécessaires — et qui ont fait leurs preuves — pour développer le cadre juridique des pays permettant d'incri-

miner les actes relevant de la cybercriminalité et d'en poursuivre les auteurs. La Convention arabe pour la lutte contre la cybercriminalité signée le 21 décembre 2010 fait de même. Elle incrimine aussi des infractions relatives au terrorisme, commises à travers un système d'information. Quant à la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel du 27 juin 2014, elle impose aux États membres la mise en place d'une politique et d'une stratégie nationales de cybersécurité. Elle est également le premier document juridique régional à imposer aux États la protection des infrastructures critiques de l'Information. Encore appelé la Convention de Malabo, le texte africain pose également les principes et règles de protection des données personnelles.

En Europe, la Directive NIS « Network Security and Information » (Réseau de sécurité et d'information), proposée en février 2013 par la Commission européenne, approuvée en décembre 2015, devrait entrer en vigueur en 2018. Cette directive traite des mesures à mettre en place afin d'assurer un niveau élevé en matière de systèmes de réseaux et d'information au sein de l'Union européenne. Elle précise également les obligations en matière de sécurité qui s'imposent aux « opérateurs fournissant des services essentiels » et aux « fournisseurs de services numériques ».

Ainsi chaque pays, selon sa culture et ses besoins, qui s'appuie sur les conventions régionales et internationales pour définir le droit pénal et le corpus de normes procédurales relatifs à la cybercriminalité qui lui conviennent, gagne du temps. Il peut bénéficier de l'expertise et de l'expérience d'autres acteurs du domaine pour les accompagner dans cette démarche. De plus, il bénéficiera d'un cadre légal national compatible avec les standards internationaux, ce qui facilite grandement la collaboration et l'entraide judiciaire internationales, aspect fondamental pour le succès des enquêtes des cybercrimes transnationaux.

Le spectre des menaces s'élargissant aussi rapidement que l'évolution des usages, des services et des infrastructures numériques, il est nécessaire que les bases légales en vigueur puissent être réévaluées périodiquement afin qu'elles puissent être toujours en phase par rapport à la réalité du terrain et adaptées en conséquence. Cela peut s'inscrire dans une démarche de veille juridique.

*Conseil de l'Europe — Convention sur la cybercriminalité (dénommée également Convention de Budapest du 23.XI.2001) — (STE n° 185) et protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE n° 185bis) europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_fr.pdf

CYBERESPACE ET DROITS FONDAMENTAUX

À l'heure actuelle, il est très difficile, voire impossible de protéger de manière technologique les données personnelles et toutes les métadonnées* générées, car elles possèdent une vie cachée qui échappe au contrôle de leur propriétaire. De plus, les services ne sont généralement pas conçus pour prendre en compte les besoins de protection des données et le besoin d'intimité numérique (protection de la vie privée). Le tableau 3 résume les différents types de données que l'utilisateur fournit consciemment à un fournisseur de service ainsi que les données qui sont collectées à son insu ou déduites de ses pratiques d'Internet. Le recueil massif de données alimente le phénomène connu sous sa terminologie anglo-saxonne de « Big Data » (ou mégadonnées en français) et contribue à la transformation numérique de la société. Des plateformes informatiques collectent, enregistrent, traitent, recoupent, échangent, exploitent et valorisent le minerai informationnel à des fins de profitabilité, de performance, d'optimisation, de prévision, d'influence, de prédiction ou encore de détection.

Tableau 3 – Les différentes sources du minerai informationnel.

Sources du minerai informationnel	Caractéristiques de la matière première que sont les données de l'utilisateur
Données livrées de plein gré par l'utilisateur	Contenus des messages, photos, formulaires remplis…
Données issues de l'observation (surveillance) des pratiques de l'utilisateur	Données comportementales liées à l'utilisation des ressources (consultation de site web, pages consultées, heure, géolocalisation, terminal d'accès, produits étudiés, vidéos visionnées, recherches effectuées, achats en ligne, articles lus...)
Données combinées (profil unifié de l'utilisateur à partir de l'interconnexion de plusieurs sources)	Données regroupées à partir de plusieurs sources en ligne (message, photos, blog, amis, contacts…) et issues du monde réel (caméra de vidéosurveillance, usages de cartes de crédit, santé, assurance…)
Données créées, déduites à partir d'inférences, d'algorithmes, de traitements informatiques	Création de nouvelles données concernant les utilisateurs via des traitements informatiques (modèles mathématiques, statistiques, probabilistes…)

Par ailleurs, les principes à la base des lois sur la protection des données personnelles sont fondés sur l'accord explicite de la personne, pour une finalité de collecte connue et précise et pour une durée déterminée. Avec le phénomène de mégadonnées (*big data*) où les données sont indistinctement collectées pour un traitement ultérieur *a priori* inconnu au moment de la collecte, il semble difficile, dès lors, d'encadrer ces nouvelles pratiques d'extraction du minerai informationnel et dont la profitabilité est conçue sur l'exploitation sans limites de cette matière première.

*Une métadonnée est une donnée servant à définir ou décrire une autre donnée (Ex. Donnée : Nom/Adresse du site web consulté ; Métadonnées : identification de l'heure de consultation, de la géolocalisation, du terminal du client).

L'Internet, la transformation digitale, la surveillance électronique, la traçabilité des activités, la collecte de données, leur exploitation, les modèles d'affaires basés sur les données personnelles ou encore l'informatique en nuage, par exemple, ne sont pas forcément compatibles avec le respect des droits fondamentaux et des libertés civiles. Les données stockées, traitées, exploitées du consommateur le sont généralement dans un pays étranger où la loi l'autorise, mais où le droit national dont l'internaute est le ressortissant ne s'applique pas nécessairement.

La protection des données personnelles est une condition préalable de l'autodétermination et de la protection de la liberté d'expression et de la dignité humaine.

Un niveau de protection des données adapté aux besoins des individus et des organisations publiques et privées est difficile à assurer. Cette situation peut contribuer, notamment, à une mise en danger de la compétitivité économique, des libertés d'expression et d'association, de déplacement (liberté de mouvement, de naviguer sur Internet), du droit à l'accès à l'information, voire à la connaissance, du droit au secret de la correspondance ou du droit à la protection de la vie privée, comme reconnu dans la Déclaration universelle des droits de l'homme de 1948* (tableau 4).

Bien que la culture des droits humains et des libertés civiles, chère aux pays démocratiques, puisse être perçue et mise en œuvre fort différemment de par le monde, il n'en reste pas moins nécessaire de contribuer à les faire prospérer et respecter au travers du cyberespace et de partager cette valeur commune, qui peut être considérée comme un levier du bien vivre ensemble, partout dans le monde.

*un.org/fr/universal-declaration-human-rights/index.html « Préambule — Considérant que la reconnaissance de la dignité inhérente à tous les membres de la famille humaine et de leurs droits égaux et inaliénables constitue le fondement de la liberté, de la justice et de la paix dans le monde… »

1948	Constats	Risques potentiels
Déclaration universelle des droits de l'homme	**Article 3** « Tout individu a droit à la vie, à la liberté et à la sûreté de sa personne. »	Mise en danger de la liberté et de la sûreté via un usage abusif ou détourné des possibilités de surveillance inhérentes aux technologies du numérique
	Article 6 et **Article 8** « Chacun a le droit à la reconnaissance en tous lieux de sa personnalité juridique. » « Toute personne a droit à un recours effectif devant les juridictions nationales compétentes contre les actes violant les droits fondamentaux qui lui sont reconnus par la Constitution ou par la loi. »	Dificile à mettre en œuvre du fait de la dimension transnationale de l'Internet
	Article 12 « … Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »	La protection des données personnelles et de l'intimité numérique ne sont pas garanties. Les atteintes à l'honneur et à la réputation peuvent être facilitées par Internet.
	Article 19 « Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considération de frontières, les informations et les idées par quelque moyen d'expression que ce soit. »	La liberté d'opinion et d'expression et le droit de ne pas être inquiété pour ses opinions peuvent considérablement être mis à mal par l'usage des technologies de l'information : censure, filtrage, blocage, surveillance…
	Article 20 « 1. Toute personne a droit à la liberté de réunion et d'association pacifiques. 2. Nul ne peut être obligé de faire partie d'une association. »	La liberté de réunion et d'association dans le cyberespace peut être considérablement restreinte. Par extension, les fournisseurs de service des TIC ne devraient pas avoir la possibilité d'imposer des conditions générales contraignant l'usager à accepter un ensemble de clauses, de services qui pourraient être comparables à l'obligation de faire partie d'une « association ».
	Article 28 « Toute personne a droit à ce que règne, sur le plan social et sur le plan international, un ordre tel que les droits et libertés énoncés dans la présente Déclaration puissent y trouver plein effet. »	La faiblesse des mécanismes de régulation internationale et le déficit de gouvernance universelle de l'Internet limitent l'expression de ce droit fondamental.
Roman de George Orwell, *1984* : « Big Brother is watching you »	**Big Brother** : dictateur invisible exerçant un contrôle totalitaire via un système de surveillance asymétrique	Procédés de surveillance asymétriques liberticides, abus de pouvoir et atteintes à la sphère privée des individus par des acteurs étatiques et non étatiques de l'Internet (entreprises privées, criminelles, terroristes…).

Tableau 4 — Internet, un nouveau *Big Brother* ?

PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Les traitements informatiques, le web, les services en ligne, s'appuient sur des données qui permettent d'identifier des personnes physiques de manière précise, de connaître leurs habitudes, ce qu'ils font, ce qu'ils achètent, ce qu'ils consomment, ce qu'ils photographient, où ils sont, ce qu'ils font, ce qu'ils aiment, ce qu'ils connaissent, etc. Les consommateurs du numérique laissent des traces électroniques à chaque usage. Des données sont collectées, le plus souvent à leur insu, par les fournisseurs de services et les divers intermédiaires techniques et opérateurs des infrastructures informatiques et de télécommunication.

Les fichiers mis en œuvre dans de tels traitements se trouvent dans de multiples systèmes de prestataires divers (centres de santé, opérateurs téléphoniques, services urbains de distribution d'électricité et d'eau, services administratifs, structures associatives, etc.) Toute cette masse d'information peut concourir à porter atteinte au respect de la vie privée des individus et à l'intimité numérique (*vie privée*), s'il n'existe pas de mesures de sécurité appropriées et un cadre juridique pour contribuer à éviter les usages abusifs et criminels de l'exploitation des données personnelles.

De plus, la personnalisation des services, la publicité ciblée, le spam, le profilage des internautes comme leur surveillance sont devenus une réalité. Le téléphone mobile en devenant intelligent (*smartphone*) et en intégrant des applications Internet (réseaux sociaux, conversations, partage de photos, vidéo…) offre la possibilité d'un lien social potentiellement infini, mais, en même temps, contribue à la surveillance de son propriétaire.

Par ailleurs, le croisement des sources d'information capables de collecter des informations relatives à une personne (caméra de vidéosurveillance – vidéo protection, réseaux sociaux, paiements électroniques, capteurs biométriques, transports en commun, cartes de fidélité, passe dans des bâtiments, etc.) permet de réaliser des corrélations et des inférences entre des informations parfois d'apparence anodine ou dénuées d'intérêt, leur conférant ainsi une valeur nouvelle exploitable à des fins commercialisables ou de surveillance.

Il est important d'assurer la protection des données à caractère personnel par des approches complémentaires relatives à :

- des actions de sensibilisation des usagers et consommateurs aux bonnes pratiques qui permettent de contribuer à la protection de leurs données et de leur vie privée et intimité numérique, à la compréhension des risques liés à un usage abusif, détourné ou criminel de leurs données personnelles ;
- un cadre juridique adapté ;
- des instances de contrôle et de suivi du respect de la protection des données personnelles et des droits fondamentaux, ainsi que des libertés civiles efficaces, notamment,

pour ce qui concerne la liberté d'expression et d'information, la liberté de naviguer librement et la liberté de réunion et d'association sur le Net, le droit au secret des correspondances, le respect de la vie privée et familiale, le droit à la dignité humaine. En plus des grandes déclarations d'intention et au-delà des structures installées, souvent dans l'urgence, il est important de veiller scrupuleusement :

- à définir le cadre de collecte et d'exploitation des données à caractère personnel ;
- à spécifier les cadres et conditions de stockage des données collectées ;
- à la délivrance des autorisations légales pour exploiter des fichiers informatiques ;
- au respect de la finalité des traitements ;
- à la sécurité des fichiers ;
- à l'obligation de communication adressée aux personnes concernées ;
- à la confidentialité des données ;
- au respect de la durée de conservation des informations.

Ces dimensions humaine et légale de la protection des données à caractère personnel, se doivent d'être complétées par des approches techniques managériales qui placent ce besoin de protection au cœur de la conception des technologies, des services et de leur gestion.

FACTEURS DE SUCCÈS DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ

Comme toute action de sécurité, la lutte contre la cybercriminalité, les cyberabus ou encore les cyberdérives est complexe. Elle doit s'inscrire dans une optique de protection des personnes, des biens matériels et immatériels et défendre les valeurs et la culture des sociétés dans lesquelles elle se réalise.

Tenter de restreindre les cyberdérives nécessite une volonté politique, une stratégie nationale de cybersécurité, des ressources et compétences, des structures organisationnelles et des procédures ainsi qu'une coordination adaptée. Cette action ne peut se réaliser sans des partenariats publics – privés et des systèmes de justice et de police efficaces au niveau national et international.

Pour ce qui concerne plus particulièrement la cybercriminalité, il importe de prendre en considération entre autres (figure 8) :

- la connaissance des acteurs du monde « cyber » et de leurs modes opératoires ainsi que de l'ampleur du phénomène (qui sont les cibles, les victimes, les vecteurs des cyberactions nuisibles ? à qui profite le « crime », l'économie illicite, les marchés noirs de la cybercriminalité ? etc.) ;
- les besoins d'entraide judiciaire internationale et les procédures réglant, entre autres, les problèmes de compétence territoriale ;
- la question de la gouvernance mondiale d'Internet.

Lutter efficacement contre la cybercriminalité passe par une approche préventive qui consiste à rendre le cyberespace plus résilient et moins favorable à l'expression de la criminalité et à réduire les opportunités criminelles. Par conséquent, il faut élever le seuil de difficulté de réalisation des cyberattaques (augmenter les coûts en termes de compétences et de ressources pour le malveillant et diminuer les profits attendus) et accroître les risques pris par les criminels d'être identifiés, localisés et poursuivis.

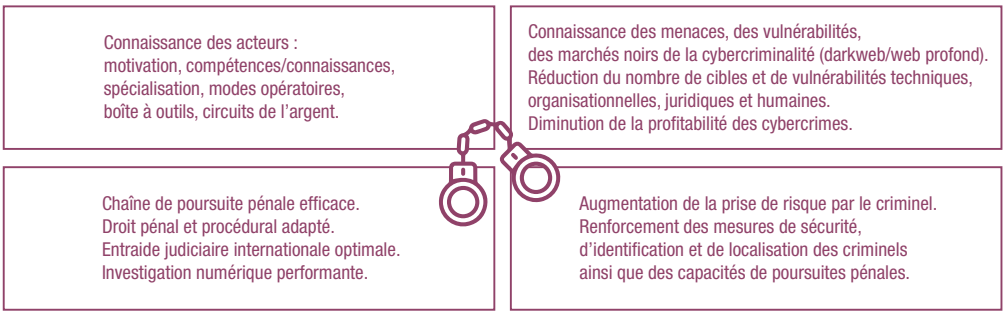


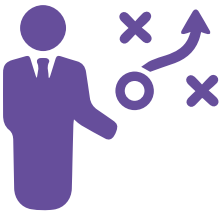
Figure 8 — Facteurs de succès de la lutte contre la cybercriminalité

Cette stratégie passe entre autres, par :

- la réduction du nombre de vulnérabilités techniques, organisationnelles, juridiques et humaines des environnements connectés à Internet ;
- le renforcement de la robustesse et de la résilience des infrastructures informatiques par des mesures de sécurité technologiques, procédurales et managériales cohérentes et complémentaires ;
- une réelle capacité d'adaptation des moyens de cybersécurité et de cyberdéfense à une situation en constante évolution ;
- l'allocation de moyens pour gérer les crises « cyber » afin de retourner à un fonctionnement normal.

Cela signifie également que ces actions doivent s'inscrire dans une volonté politique forte et un engagement des États à :

- faire de la lutte contre la cybercriminalité et du renforcement des capacités de cybersécurité et de cyberdéfense une priorité ;
- renforcer la coordination entre les différents États et gouvernements de la Francophonie ;
- respecter les droits fondamentaux des personnes ;
- mettre en œuvre des mesures appropriées et proportionnées aux menaces ;
- mobiliser, fédérer et engager les différents acteurs privés du numérique et de la société civile autour de la lutte contre la cybercriminalité et le développement de la cyberdéfense.



STRATÉGIE NATIONALE

JUSTIFICATION

Tous les pays sont dorénavant confrontés à de nouveaux risques induits par l'usage extensif des technologies de l'information et de la communication. Le taux de pénétration de l'Internet tend à se stabiliser dans les pays industrialisés, mais il connaît une forte croissance dans les pays émergents ou en développement, notamment du fait du déploiement d'infrastructures et de l'accès grandissant aux services de la téléphonie mobile. L'usage du numérique, que cela soit à des fins professionnelles ou privées, sous-tend tous les processus de modernisation de l'État et offre de nouvelles opportunités pour le développement économique et personnel.

Le numérique est un marché à part entière et un moteur de croissance. Toutefois, tous ses potentiels de profitabilité, pour ceux qui le maîtrisent, sont à revisiter au regard des nouveaux risques qu'il induit. Le développement numérique engage les dirigeants politiques des pays à relever de nouveaux défis d'ordre politique, économique, juridique et social pour maîtriser les cyberrisques engendrés.

Chaque pays doit apporter une réponse globale et coordonnée au besoin de gouvernance et de pilotage de la cybersécurité et de la cyberdéfense afin de maîtriser ses infrastructures numériques, protéger ses valeurs, son économie et sa population et garder les cyber risques sous contrôle, c'est-à-dire à un niveau acceptable. Une approche régionale peut aussi être envisagée si des pays, ayant le même type de problèmes, d'infrastructures, de besoins, cherchent à optimiser leurs efforts et leurs investissements.

DÉMARCHE

Le premier pas de la maîtrise des cyberrisques passe notamment par :

- la définition d'une stratégie nationale de cybersécurité ;

- la mise en place d'un plan d'action (véritable feuille de route de la réalisation de la stratégie cyber) ;
- la création de structures organisationnelles de support (centre d'alertes, de détection et de réponse aux cyberincidents, de gestion de crises, centre de formation et de sensibilisation, centre de coordination nationale/régionale, centre de coopération et de relations internationales, centres de recherche…) ;
- la mise en place ou l'amendement d'un cadre légal approprié (bases juridiques, lois sur la protection des données, sur l'identité numérique, sur les infractions rendues possibles par le numérique…).

Une stratégie nationale de cybersécurité peut avoir comme principaux objectifs de renforcer la robustesse et la résilience des infrastructures numériques, la prévention des menaces et leurs détections précoces qu'elles soient liées à des catastrophes naturelles, des erreurs, ou à des actions malveillantes ; ce qui inclut en particulier la lutte contre la cybercriminalité et les usages abusifs de l'informatique.

La Stratégie nationale devra refléter l'importance économique de la cybersécurité. Elle doit :

- identifier les services critiques à sécuriser et à rendre résiliants ;
- définir une autorité compétente avec des attributions claires et bien délimitées ;
- identifier les entités (gouvernement et secteur privé) impliquées dans la mise œuvre de la Stratégie et clarifier leurs rôles ;
- identifier les ressources humaines et économiques requises ;
- identifier les mécanismes de sécurisation des infrastructures critiques et comment les mettre en œuvre.

La protection des infrastructures critiques, c'est-à-dire essentielles ou vitales au bon fonctionnement de la société (électricité, transport, approvisionnement alimentation, eau, télécommunication, finance, fonctionnement du gouvernement…), fait également parti des besoins de sécurité à prendre en compte dans une stratégie nationale de cybersécurité, puisque ces infrastructures peuvent faire l'objet de cyberattaques et que l'informatique dont elles dépendantes les ont exposés aux cybermenaces.

CYBERSÉCURITÉ ET CYBERRÉSILIENCE

Que ce soit dans le domaine de l'écologie, de la psychologie, du management, de l'informatique ou de l'économie par exemple, la résilience est relative à la capacité d'un « système » à pouvoir continuer à opérer, si possible normalement après un incident, un choc, une perturbation, une panne.

Parler de cyberrésilience aujourd'hui, revient à admettre qu'il est impossible d'empêcher des cyberincidents d'advenir, que le cyberespace est un monde fragile, instable et potentiellement hostile. Pour autant, faire de la cyberrésilience ne revient pas à accepter une relative impuissance à protéger correctement les infrastructures informationnelles, même si parfois il peut exister une certaine insuffisance de mesures de sécurité préventives efficaces (tableau 5).

La cybersécurité ne doit pas s'inscrire uniquement dans une logique de réactivité qui permet d'être préparé à « survivre » à un cyberincident d'origine intentionnelle ou non. Bien que cette capacité à résister soit fondamentale et absolument nécessaire, elle ne peut suppléer à un défaut d'une approche globale multiacteurs aux niveaux national et international, à l'appréhension du phénomène relevant pour l'essentiel de la cybercriminalité et de la réalité des cyberattaques.

Cyberrésilience	Capacité d'un « système » à pouvoir continuer à opérer normalement après un incident.
Cybersécurité	Ensemble de mesures stratégiques et opérationnelles permettant à un système de fonctionner.

Tableau 5 — Complémentarité des approches de cyberrésilience et de cybersécurité.

CYBERDÉFENSE

CYBERESPACE : UN TERRAIN D'OPÉRATIONS MILITAIRES

Le cyberespace est un nouvel espace où se déploient toutes sortes d'activités. Il permet entre autres, d'influencer, de déstabiliser ou encore de réaliser des profits. C'est un instrument au service de la profitabilité économique et un lieu d'expression du pouvoir : en fait, un territoire stratégique*. Dès lors, il est à protéger et à défendre. De plus, comme dans tous les secteurs d'activité, les activités militaires sont, elles aussi, tributaires de l'informatique et des systèmes d'information pour être opérationnelles et performantes. L'efficacité des moyens de défense traditionnelle dépend désormais des capacités informatiques. Le Sommet de l'OTAN de juillet 2016 à Varsovie** a d'ailleurs réaffirmé que le cyberespace est désormais considéré comme le cinquième champ de bataille et qu'à ce titre il est un terrain d'opérations militaires au même titre que la terre, l'air, l'espace ou la mer.

De plus, les forces de défense d'un pays, son armée, doivent pouvoir s'appuyer sur des infrastructures informatiques sécurisées. Il est donc primordial, au-delà de pratiquer la guerre par des moyens informatiques (actions militaires dans le cyberespace, notions de guerre informatique, de cyberguerre, d'informatique offensive et défensive), que le « secteur de la défense » puisse assurer la sécurité de ses infrastructures informatiques et de télécommunication, au même titre que n'importe quelle infrastructure critique. L'objectif d'une armée opérationnelle tant sur le plan stratégique que sur celui des opérations militaires, constitue le premier objectif de la cyberdéfense d'un pays, qui peut être complété par celui de pouvoir être en mesure de défendre son pays, sa population et son économie, en cas de conflit. Les besoins de cyberprotection, d'assistance aux autorités civiles, de renseignement, de logistique, de cy-

L'écosystème numérique construit autour d'Internet et des réseaux informatiques constitue un domaine où le secteur de la défense est présent. Par conséquent, toute doctrine militaire se doit impérativement de prendre en compte cette nouvelle dimension d'expression du pouvoir militaire.

*S. Ghernaouti ; « Cybercriminalité : le visible et l'invisible ». Le savoir suisse, Presses polytechnique et universitaire romandes, 2009.

** nato.int/cps/fr/natolive/index.htm — nato.int/cps/fr/natohq/official_texts_133169.htm

berdéfense passive et active comme les missions et rôles de l'armée doivent être clairement exprimés et pris en compte dans une stratégie nationale de cyberdéfense pour dégager les moyens nécessaires à la gouvernance et à la réalisation d'une cyberdéfense efficace.

Faire aujourd'hui des choix d'une politique de cyberdéfense, c'est conditionner et contraindre les choix stratégiques et opérationnels de demain, d'où l'importance accrue à comprendre en quoi les technologies du numérique modifient structurellement et sur le long terme le monde dans lequel nous vivons et de réaliser des études prospectives de gestion de risques.

INTERNET ET LE CODE INFORMATIQUE AU SERVICE DU POUVOIR

Internet et les réseaux informatiques constituent, pour les forces armées, un moyen de projeter du pouvoir, en déployant des forces informatiques hors de ses frontières géographiques. Ainsi, le code informatique et les programmes peuvent être considérés comme des guerriers électroniques, contrôlables à distance, permettant de contraindre l'ennemi via des cyberattaques et d'intervenir dans des cyberterritoires étrangers sans déclarer officiellement la guerre aux adversaires ciblés par des actions d'informatique offensive ou défensive. Le cyberennemi est plus qu'un système informatique, car derrière chaque équipement, il peut y avoir des cibles civiles, économiques, humanitaires et/ou militaires.

Toutefois, l'expression de la force, de la puissance et de domination de certains acteurs ou pays dans le cyberespace, passe par leurs capacités à maîtriser leurs infrastructures physiques et environnementales de l'Internet, l'accès à Internet (rétrospectivement l'interdiction d'accès), par la maîtrise des noms de domaine et des adresses, des contenus et des données, mais aussi par la maîtrise des flux et des mouvements ainsi que de la géolocalisation.

Depuis quelques années, la notion de cyberguerre est souvent évoquée, lorsque des attaques informatiques ciblent des infrastructures critiques des pays, des systèmes industriels, ou encore lorsque des impacts de déstabilisation économique graves en résultent (attaques contre l'Estonie en 2007, Stuxnet en Iran en 2010 par exemple).

Chaque pays est désormais confronté à faire face à des cybermenaces émanant d'acteurs étatiques ou non et qui peuvent porter atteintes à sa sécurité et sa stabilité. Les cyberattaques font partie de l'arsenal militaire permettant de faire la guerre par des moyens non militaires. Elles peuvent constituer à elles seules l'expression de conflits, mais peuvent aussi accompagner tout conflit « classique ». L'imbrication du virtuel et du réel, le continuum cyberphysique ont favorisé l'émergence de la notion de guerre hybride s'exécutant sur des territoires réels et au travers du cyberespace via Internet et tous les réseaux informatiques et de télécommunications.

De manière générale, la cyberguerre est une guerre de l'information, par l'information (ou le code informatique) et pour l'information. Toute action politique, tous les conflits font l'objet d'une grande médiatisation sur Internet, et il en va du marketing de la guerre comme de toute autre action commerciale. Cela peut s'exprimer également sous la forme de guerre psychologique ou de guerre sémantique de manipulation de l'information, pour influencer, déstabiliser, manipuler l'opinion publique, influencer les prises de décisions de chacun y compris des dirigeants économiques et politiques.

CAS PARTICULIERS

Le monde terroriste a bien compris les avantages stratégiques qu'il pouvait tirer de la maîtrise de l'information et de l'image, de l'utilisation de toutes les capacités de communication et de mise en relation qu'offre Internet. Ainsi, le cyberespace offre une caisse de résonnance mondiale à leurs actions, à leur propagande et autorise entre autres, recrutement, endoctrinement, formation, préparation d'actions terroristes, levées de fonds, etc. Aussi la lutte contre le terrorisme et la prévention de la radicalisation violente passe par des actions menées également dans le cyberespace.

Par ailleurs, des activistes peuvent s'exprimer avec des cyberattaques (notion d'hacktivisme composé des mots hacker et activiste), notamment en recrutant via Internet des vecteurs de propagation d'attaques en déni de services sur certaines cibles emblématiques, ennemies des causes qu'ils défendent (c'est par exemple le cas des actions menées par des communautés d'internautes anonymes connus généralement sous le vocable Anonymous).

Il faut être prudent dans la catégorisation des actions et de leurs auteurs, car cela dépend fortement du contexte et de l'environnement géopolitique dans lequel ces derniers opèrent. Ils peuvent, tout à la fois, être vus par certains, comme des résistants, des dissidents et par d'autres, comme des lanceurs d'alerte, des défenseurs des droits humains et libertés civiles, des dénonciateurs de dysfonctionnements ou de corruption, par exemple. En effet, Internet permet de faire émerger de nouvelles formes de participation citoyenne, de contrôle démocratique et d'alertes. Certains gouvernements l'ont bien compris et développent la participation citoyenne, des consultations publiques, voire même des processus d'évaluation de leurs actions auprès de leurs administrés à des fins d'amélioration.

Internet est devenu non seulement un outil de la performance économique des acteurs licites, mais il est également au service de la performance criminelle (crime économique, trafics d'armes, de stupéfiants, d'êtres humains…), de la performance terroriste et de la performance militaire.

CYBERPAIX — CYBERSTABILITÉ

Chaque pays doit dans sa posture militaire intégrer une stratégie et des mesures opératives lui permettant non seulement de développer la robustesse et la résilience de ses infrastructures numériques, mais aussi de pouvoir démontrer ses capacités de cyberdéfense et de cyberdissuasion afin de contribuer à la paix et à la stabilité internationale, à la prévention des conflits et à la protection de sa population, de l'intégrité de ses cyber territoires, de ses biens et valeurs (figure 9).

Cette posture de défense peut être renforcée par une bonne capacité d'anticipation stratégique qui s'appuie sur la maîtrise de l'information stratégique, des processus de renseignement et d'intelligence ainsi que sur celle des technologies de l'information et de la communication et d'Internet. Ceci revient à pouvoir assurer et maintenir un niveau de cybersécurité efficace des infrastructures numériques et des réseaux de télécommunication et à pouvoir, le cas échéant, répondre à des cyberattaques d'envergure.

Faire face à des cyberattaques suppose suppose une organisation, une préparation, des outils, des compétences, des processus, mais aussi des entraînements et des exercices de simulation de gestion de crises et de réaction à des cyberattaques.

Pour un pays, avoir un secteur de la défense possédant une vision stratégique de la cyberdéfense ainsi que des capacités opératives pour contrer des cybermenaces et réagir aux cyberattaques est fondamental, comme le sont d'ailleurs ses capacités à pouvoir au niveau civil, se prémunir des cyberincidents qui menacent ses institutions publiques et privées ainsi que ses ressortissants, ce qui comprend entre autres, ses capacités à lutter contre la cybercriminalité.

Cela suppose également une vision politique, une stratégie nationale de cybersécurité (ou de lutte contre les cyber risques) qui se traduit, dans les faits, par une efficacité et efficience opérationnelle au travers de :

- structures organisationnelles cohérentes ;
- un cadre juridique adapté ;
- capacités de surveillance et de renseignement ;
- compétences humaines réelles ;
- un ensemble cohérent de ressources organisationnelles, managériales, juridiques, technologiques, procédurales, budgétaires complémentaires, correctement dimensionnées, évaluées et optimisées ;
- partenariats public — privé fédérés autour d'un intérêt commun, tout en autorisant la préservation des intérêts de chacun.

Développer des axes stratégique, tactique et opérationnel dans les domaines de l'informatique offensive et défensive ainsi que celui de la gestion de crise informatique est donc incontournable. Certains pays l'ont bien compris et sont très actifs dans ce domaine et dans la conquête et la domination du cyberespace. Rappelons que le Département de la Défense américain (DoD) est à l'origine d'Internet, que depuis toujours l'informatique, la cryptographie, les techniques de géolocalisation sont au service des forces armées.

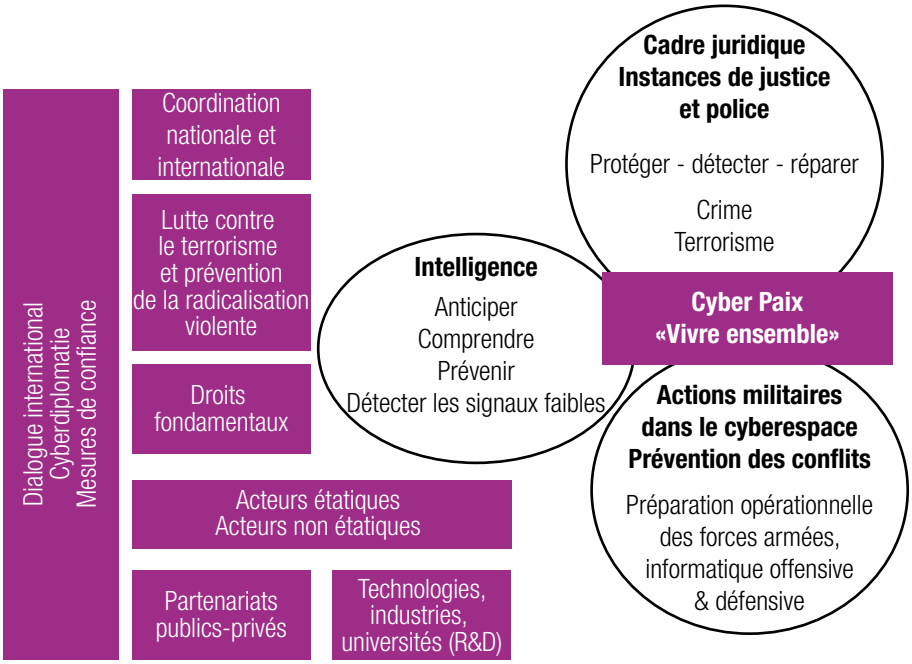


Figure 9 — Éléments de cybersécurité et de cyberdéfense

COMPLÉMENTARITÉ DES STRATÉGIES NATIONALES DE CYBERSÉCURITÉ ET DE CYBERDÉFENSE

Accuser un retard en matière de doctrine informatique offensive et défensive, sous prétexte de ne pas vouloir alimenter un discours sur « la militarisation » de l'Internet, serait faire preuve de naïveté et d'angélisme et desservirait la société en laissant d'autres entités imposer leur suprématie dans le cyberespace et dans le monde réel.

L'imbrication et les interdépendances des mondes civil et militaire, au travers du cyberespace, nécessitent de penser les problématiques de cybersécurité et de cyberdéfense comme un continuum civilo-militaire (figure 10). De la pertinence des partenariats et mode de coopération civilo-militaire, de la collaboration d'acteurs industriels des tech-

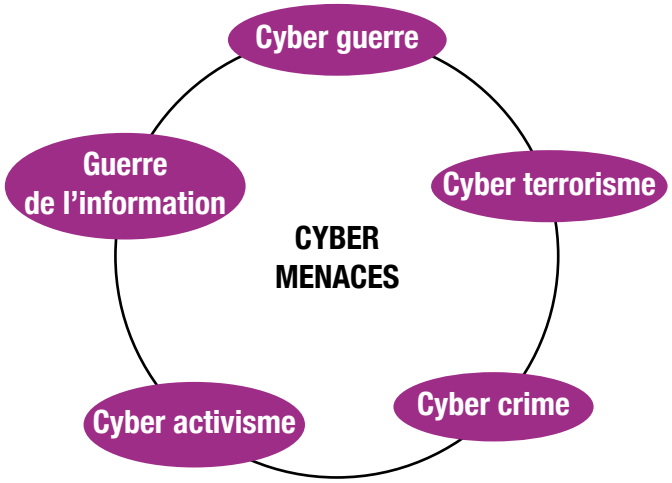


Figure 10 — Nécessité d'une approche intégrée pour faire face aux cybermenaces.

nologies du numérique et des agences étatiques de défense dépend le niveau de sécurité de la sécurité globale d'un pays. Il est donc primordial de penser conjointement, afin d'éviter la duplication des efforts et des ressources, mais surtout pour assurer une bonne coordination et un niveau de cohérence et de performance adéquats aux actions de sécurité et de défense. Autrement dit, il est important de développer un continuum de cybersécurité et cyberdéfense cohérent. Cette approche vise également à soutenir des forces militaires avec des moyens civils.

Doctrine et posture de cyberdéfense se développent, notamment dans les pays les plus connectés. Elles reposent sur des acteurs formés à la cybersécurité et à la cyberdéfense, ce qui suppose que de telles filières de formation existent. Par ailleurs, un réservoir de miliciens ou de réservistes éventuellement civilo-militaires, dûment accrédités et compétents en cybersécurité, peut contribuer à la cyberdéfense d'un pays. Une connaissance approfondie des systèmes, des vulnérabilités, une attitude vigilante, une fonction de renseignement, une veille active et dynamique de l'environnement cyber, ancrées dans la réalité politique du moment, contribuent à avoir une approche prospective pour mieux anticiper les menaces, maîtriser les risques cybernétiques, détecter les anomalies pour en limiter les impacts et développer la cyberrésilience.

Résister aux cyberattaques est désormais une responsabilité collective.

On se doit de réinventer la coopération civilo-militaire, pour offrir un continuum de sécurité – défense cohérent à la population et à la société (Figure 11).

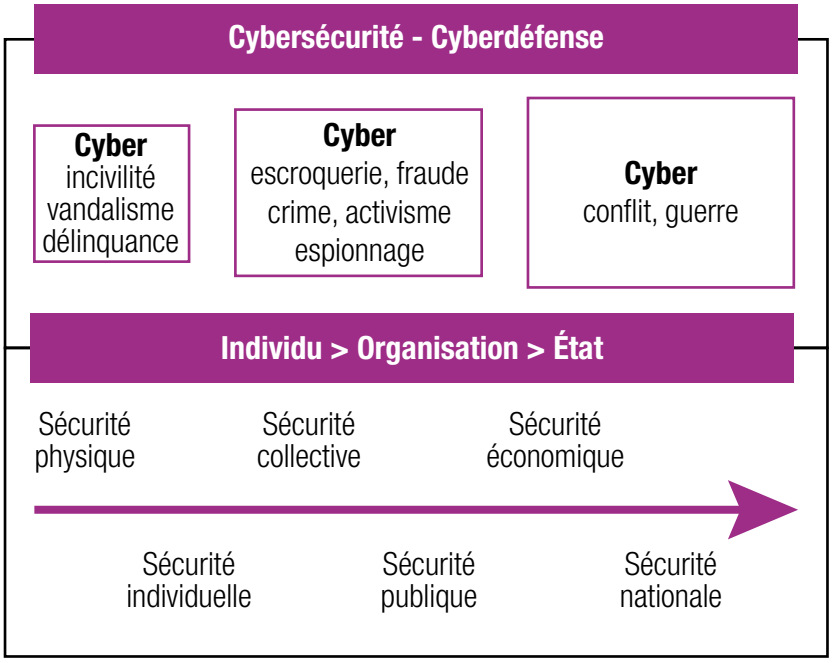


Figure 11 — Le continuum de la sécurité.

La cybersécurité ne peut s'appréhender que de manière interdisciplinaire et intégrative. Cela se traduit au niveau de l'État par une vision partagée et transversale de la problématique et par une collaboration interministérielle (interdépartementale, inter-office) renforcée et par une capacité à travailler ensemble.

LE CYBERSPACE : UN ESPACE COMMUN À PARTAGER ET À RÉGULER*

Le cyberespace avec lequel nous interagissons pourrait être considéré comme un espace global commun dont les frontières seraient liées à la localisation géographique des individus qui l'utilise et à celle où est implantée l'infrastructure physique de support. La notion de propriété ainsi que l'existence d'un cadre légal applicable peut également permettre de délimiter le cyberespace. Toutefois, sa couverture internationale, son usage extensif par un nombre toujours croissant de la population de par le monde, notamment au travers des applications de la téléphonie mobile, et la dépendance de plus en plus forte des sociétés aux infrastructures numériques, obligent à penser collectivement et globalement aux niveaux national, régional et international son développement, son utilisation, son partage et sa régulation. Effectivement, il serait préjudiciable à la stabilité des pays que le cyberespace soit uniquement un champ de bataille économique et militaire, reflétant toutes sortes de conflits ou de compétitions économiques et politiques.

Bien qu'il soit le fruit d'une évolution technologique qui s'inscrit dans un contexte géopolitique particulier, et qu'à ce titre il ne peut être considéré comme une évolution naturelle, le cyberespace n'est pas complètement comparable à la terre, la mer, l'air et l'espace.

Toutefois, comme ces éléments naturels, il doit être partagé et donc régulé. Le cyberespace requiert des mesures de coordination, de coopération et des mesures légales applicables au niveau local, mais aussi effectives et compatibles au niveau international. Ainsi, un instrument de contrôle supranational inscrit dans le cadre des Nations Unies devrait exister et être applicable.

Une telle œuvre contribuerait à spécifier les pratiques acceptables et à poursuivre les délits, quel que soit leur lieu de réalisation. De plus, cela devrait permettre de faire en sorte que des crimes portant atteinte à la paix et à la sécurité, au travers d'Internet, deviennent punissables par le droit international, même s'ils ne sont pas répréhensibles à un niveau national.

*Paragraphe adapté de S. Ghernaouti ; « Les cyberrisques : réalités et perspectives » ; SCARG 2013. ISDN 978-2-97-0087809.

Dans la mesure où l'Internet possède une couverture mondiale et que les cybermenaces et les cybercrimes ne s'arrêtent pas aux frontières d'un pays ou d'une région, des accords régionaux ou bilatéraux ne sont pas suffisants. Des outils juridiques plus larges sont donc nécessaires.

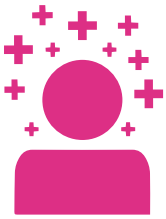
Ainsi, un accord international faciliterait :

- la compréhension commune de tous les aspects de la cybersécurité ;
- une harmonisation et une complémentarité des mesures stratégiques et opérationnelles nationales ;
- le développement d'une stratégie globale de prévention, de dissuasion et de réaction contre des cyberattaques ;
- le partage d'information et l'alerte précoce d'incidents.

Porté par la communauté internationale, un Traité du cyberespace* devrait pouvoir être élaboré dans le cadre des Nations Unies, pour traduire une volonté politique et économique forte et un engagement réel de tous les pays. L'élaboration d'un tel traité fait l'objet de débat au sein de la communauté internationale, et prendra du temps. Seul un dialogue international honnête et loyal autour d'un partage d'intérêts communs contribuera à fixer les règles du bien vivre-ensemble dans le cyberespace, d'identifier les limites des pratiques acceptables et celles qui ne le sont pas et de dénoncer les usages abusifs ou criminels ainsi que leurs auteurs. Conscient qu'un traité n'est pas un frein à la cybercriminalité ou à l'expression des conflits dans le cyberespace, il n'en est pas moins nécessaire pour faire prendre conscience qu'il ne s'agit plus d'imposer la loi des acteurs les plus forts dans le cyberespace. À la manière d'un protocole international concernant le climat, il pourrait exister des lignes directrices du développement du cyberespace que nous allons laisser en héritage aux générations futures et de baliser ensemble la voie à suivre en tenant compte de tous les acteurs concernés, pour une certaine écologie du cyberespace. Ce processus est long, mais permet aussi de sensibiliser la population ainsi que ces dirigeants économiques et politiques aux cyber risques et de leur rappeler leurs responsabilités. Nous connaissons tous les limites des traités internationaux, des problèmes liés à leur ratification et à leur respect, toutefois, ils ont quand même une utilité et efficacité passive, en fixant un cadre de référence.

Agir ensemble, en toute connaissance des risques pour saisir les opportunités technologiques afin de construire une société de l'information inclusive, bâtir un cyberespace et un écosystème numérique de confiance et durables, donner du sens aux changements induits par le numérique, devrait nous mobiliser autour d'un objectif commun et des valeurs partagées de société. Cela pourrait peut-être se résumer par la volonté de vivre ensemble en toute sécurité et stabilité dans un monde en ligne et hors ligne.

*Pour plus d'information voir : « A global treaty on cybersecurity and cybercrime ; A contribution for peace, justice and security in cyberspace », Second edition, 2011. Stein Scolberg & S.Ghernaouti-Hélie. cybercrimelaw.net/Cybercrimelaw.html



RENFORCEMENT DES CAPACITÉS ET CAPITAL HUMAIN

Comme c'est le cas pour toute initiative d'envergure nationale, la cybersécurité et la cyberdéfense requièrent de disposer d'une imposante force en capital humain. Cette force doit être diversifiée et au meilleur de ses capacités.

Dans le cas spécifique du renforcement des ressources humaines dédiées à la cybersécurité et à la cyberdéfense, l'objectif est de construire des parcours professionnels associés à de l'expertise de haut niveau. Les expertises ainsi mises à disposition de l'écosystème numérique devront remplir plusieurs fonctions :

- participer à la connaissance et à l'anticipation de la menace cyber et à la maîtrise des risques ;
- soutenir la lutte contre les cyberattaques, notamment dans le contexte de la lutte contre la cybercriminalité, la protection des infrastructures critiques et des équipements des structures d'importance vitale ;
- offrir les outils et les connaissances nécessaires à toute la chaîne des acteurs de la justice pénale dans le domaine de la lutte contre la cybercriminalité ;
- collaborer au développement et à l'évaluation de produits et solutions de cybersécurité et de cyberdéfense ;
- participer à l'ingénierie de la cybersécurité, en particulier dans le domaine de la conception et lors de la mise en œuvre de moyens techniques (chiffrement, pare-feu, détection d'incidents, ...) ;
- apporter les processus, procédures et contrôles nécessaires à la gouvernance, à la gestion opérationnelle, à l'évaluation et à l'optimisation des mécanismes de sécurité ;
- proposer le soutien nécessaire à la prise en compte et à la satisfaction des besoins juridiques et managériaux et d'intelligence économique ;
- encourager des actions de sensibilisation et de formation de la population ;
- contribuer à l'animation et au développement de la recherche et de la formation, en assurant le lien entre les centres de formation et de recherche et les entités de l'économie numérique pour innover, créer de la valeur et contribuer à résoudre les

problèmes auxquels la société est confrontée ;
- organiser des exercices de simulations bilatérales et régionales de réponse aux menaces et aux attaques dans les secteurs de la cyberpolice, de la cybersécurité et de la cyberdéfense ;
- développer les cursus de formation académique et professionnelle afin de mettre rapidement sur le marché les compétences indispensables.

En vue de gagner ce défi de la disponibilité en qualité et en quantité suffisantes des compétences spécifiques pour la cybersécurité et la cyberdéfense, il est important d'offrir des mesures incitatives aussi bien aux centres de formation qu'aux futurs apprenants. Les avantages financiers à offrir des formations pointues en cybersécurité et cyberdéfense et les incitations à s'engager dans de telles formations doivent être explicites. Il s'agira de renforcer la formation et la pédagogie envers les entreprises, les centres de formation et tous les acteurs (techniciens, développeurs, ingénieurs, manageurs, juristes…), afin d'accompagner la promotion de la cybersécurité et de la cyberdéfense.

De plus, la création de cours en ligne ouverts et massifs francophones (CLOM) avec des contenus et des modules de formation en langue française devrait pouvoir contribuer au développement des capacités humaines, mais aussi au développement et à la promotion d'une culture francophone de la cybersécurité et de la cyberdéfense. Cela peut s'appuyer sur des programmes de jumelage et d'échange entre institutions académiques francophones, en particulier pour des programmes de masters. Cette démarche comprend également des actions visant à favoriser et soutenir les échanges entre les centres de recherche et les universités dans le domaine de la cyberdéfense et de la cybersécurité et a développer une intelligence et une excellence francophone dans ces domaines.

Les mesures incitatives peuvent prendre la forme de subventions aux organismes, aux universités ou aux entreprises, de bourses d'études, etc. La participation active des fonds de promotion d'emploi et de création d'entreprises est ici aussi indispensable.

Cet ensemble de mesures incitatives ouvre un champ d'opportunités aussi bien pour les individus que pour le secteur privé. Il est indispensable que ce secteur privé se saisisse rapidement de cette nouvelle donne pour transformer les initiatives gouvernementales en activités pérennes. Qu'il s'agisse de laboratoires d'expérimentation, de centres d'accréditation ou de centres de certification, ce sont là autant de niches qui ont démontré leurs valeurs dans les changements technologiques. Il appartient aux structures de formation, aux entreprises privées, aux divers prestataires de services d'œuvrer à la mise en place de cet environnement d'accompagnement de la qualité.

Former des personnes compétentes de très haut niveau est une composante de cette nécessité de l'édification d'une force cyber. Mais après la formation, il faut assurer des parcours professionnels attractifs et évolutifs, le recrutement et les mobilités de carrière de ces personnes, notamment au sein des agences gouvernementales, afin que l'État, puisse bénéficier également des talents dans le domaine cyber, s'approprier les innovations technologiques qui concourent au progrès social et économique.

La construction des capacités en matière de cybersécurité doit s'appuyer sur un socle d'une éducation de base en informatique et en culture du numérique dont les principaux points sont rappelés par le tablea ci-dessous :

Développer des programmes de sensibilisation	Introduire le numérique dans l'enseignement de base et au secondaire. Généraliser l'apprentissage du numérique dès le plus jeune âge. Faire de tous les élèves des cybercitoyens conscients et préparés aux opportunités et aux risques.
Rendre obligatoire la certification en cybersécurité pour les postes sensibles	Gouvernements, institutions ou entreprises nationaux et entreprises critiques pour la sécurité nationale.

Tableau 6 — Faire de l'éducation numérique et de l'informatique, la base pour la cybersécurité

Dans l'idée de progrès et d'amélioration des conditions de vie de ses ressortissants, le tableau 7 résume quelques principes directeurs, qu'un État pourrait s'approprier pour développer ses capacités en matière de cybersécurité et de cyberdéfense et contribuer à bâtir l'avenir.

1	Les États ont le devoir de protéger leurs citoyens contre les menaces liées à la cybercriminalité.
2	Les données à caractère personnel des citoyens doivent être protégées.
3	L'État de droit en ligne et hors ligne doit être garanti sans distinction aux citoyens.
4	Les infrastructures vitales au fonctionnement des services de l'État et des entreprises doivent être protégées de manière efficace.
5	Les acteurs économiques de l'industrie du numérique ainsi que la société civile doivent être associés pleinement à la lutte contre la cybercriminalité.
6	Les actions de prévention et de lutte contre la cybercriminalité ne doivent pas se faire au détriment des droits fondamentaux.
7	Les actions de prévention et de lutte contre la cybercriminalité devront être réalisées sous le contrôle des autorités judiciaires (juges et magistrats).

Tableau 7 — Principes directeurs contribuant à la maîtrise des cyberrisques

Dans une optique de rationalité et d'optimisation économiques, la figure 12 présente les différents aspects de l'intérêt de la mutualisation des ressources au sein de la francophonie.

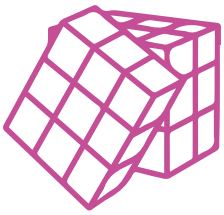
Développer et diffuser des kits francophones de formation
- dans les domaines juridique, technique et organisationnel
- organiser des ateliers de formation au niveau national et régional

Encourager les coopérations bilatérales et régionales
- exemple : la mise en œuvre de la cyberconvention africaine sous l'égide de l'Union africaine

Promouvoir les outils basés sur les standards ouverts pour
- des raisons de sécurité et d'autonomie
- faciliter le partage

Encourager l'émergence ou le développement de regroupements francophones professionnels
- promotion du savoir-faire francophone
- encourager la naissance d'un espace francophone d'affaires

Figure 12 — Mutualisation des ressources



DÉFIS ACTUELS ET FUTURS

CONSTRUIRE LA CONFIANCE

Afin d'éviter que la société de l'information se transforme en une société de la défiance et de la surveillance, il est également urgent d'apporter des réponses convaincantes à la nécessité de pouvoir construire la confiance dans le cyberespace et de proposer des solutions de protection fiables, notamment pour ce qui concerne l'identité numérique des individus.

Toutes les activités et pratiques utilisant l'informatique sont génératrices de données. Ces dernières sont stockées, traitées, exploitées, corrélées, communiquées par de nombreux acteurs, sans pour autant que les propriétaires légitimes de ces données en soient forcément conscients ou même soient consentants (« le réseau » n'oublie jamais et les données ont une vie cachée). Il semble désormais urgent de s'interroger sur le phénomène de « massification* » des données et sur le marché qui en découlent ainsi que le pouvoir conféré aux acteurs qui les possèdent afin de maîtriser les risques pour les individus et la société.

GÉNÉRER DE LA SÛRETÉ ET DE FIABILITÉ

Par ailleurs, nous sommes en train de construire un monde de la connectivité permanente, de la mobilité, de la communication sans fil et sans contact**, un monde où les objets deviennent intelligents et communicants : c'est l'Internet des objets. Ainsi, les objets courants (des voitures, des feux de signalisation, par exemple) intègrent des composants informatiques et des technologies de l'Internet. Ils sont alors capables d'une certaine autonomie et prise de décisions du fait d'une intelligence embarquée dans des programmes informatiques. Ces objets commencent à envahir l'espace public et de facto constituent des cibles potentielles de la cybermalveillance, car toute entité connectée à Internet est piratable. Plusieurs actions de prise de contrôle à distance de voitures sans chauffeurs ou de réfrigérateurs connectés ont d'ailleurs déjà été réalisées. De plus ce n'est pas un uniquement un système

*Notion de *Big data*.

**Le sans contact fait référence aux technologies NFC (*Near Field Communication*).

que nous connectons à Internet, ce sont nos vies que nous branchons, via notamment des téléphones portables ou des appareils de quantification de soi. Tous les objets et capteurs embarqués, puces RFID ont la possibilité de collecter des données et de les transmettre à des fournisseurs de services. Cela peut porter atteinte à la protection des données personnelles et à l'intimité des personnes en relation avec de tels objets. De plus, leur défaut de sécurité ou de robustesse, la possibilité qu'ils puissent être manipulés par des entités malveillantes ou déloyales, peut entraîner des conséquences préjudiciables à la sécurité physique des infrastructures et des personnes qui en dépendantes.

Toujours dans le registre de l'assistance aux personnes et aux activités de la vie courante, des robots plus ou moins sophistiqués commencent à partager le quotidien de certains. Capables d'influencer nos comportements et notre environnement, leur prise de contrôle par des entités déviantes ou malveillantes serait préjudiciable.

Le 21e siècle est celui des puces électroniques RFID (*Radio Frequency Identification*) et des nanotechnologies (notion de poussières intelligentes). La convergence entre le monde de l'électronique et du monde biologique est de plus en plus effective, notamment du fait de divers capteurs, prothèses, équipements électroniques biomédicaux implantés dans le corps humain pour pallier certaines de ses défaillances (pompe à insuline, pacemaker…). Si la tendance se confirme d'intégrer de plus en plus d'équipements électroniques dans des corps biologiques et ainsi d'envisager une évolution de l'être humain vers un être hybride, personne aux capacités augmentées par des technologies du numérique, comme le préfigure le courant du transhumanisme, les exigences de sécurité deviennent alors primordiales et doivent être prise en compte dès la conception de ces technologies dont dépendrait sur le long terme la survie de l'humanité. À défaut, la notion d'humain augmenté pourrait se traduire en humains faillibles et à la merci de ceux qui maîtrisent le pouvoir de les contrôler à distance, de les piloter, de les activer et de les détruire.

Des interfaces neuronales existent déjà et permettent d'interagir avec des ordinateurs par la pensée. Si cela permet de contribuer au mieux-être de certaines personnes notamment handicapées, à terme leur usage généralisé, la plus grande intégration et intrication du biologique et de l'électronique, le détournement de leur usage initial, conduirait à des actions de « piratage » informatique y compris de la pensée humaine.

METTRE DES LIMITES À DES POTENTIELS ILLIMITÉS

Ces nouveaux risques nous obligent à réinventer la sécurité afin de les maîtriser au mieux et préserver les valeurs auxquelles nous accordons de l'importance et qui sont mises en danger par la technologisation de la société.

Ainsi, dans ce nouveau contexte du tout informatisé et des nombreuses dépendances et interdépendances des êtres vivants et de toutes les activités dont notre survie est liée, que cela soit par exemple, pour ce qui concerne les chaînes d'approvisionnement, l'agriculture, l'industrie chimique, l'industrie de la santé, les transports, l'énergie, ou encore l'accès aux ressources cruciales comme l'eau potable, les enjeux de la lutte contre les cybermalveillances vont bien au-delà de la lutte contre le crime économique et la maîtrise des risques financiers. C'est pour toutes ses raisons qu'il est crucial de savoir et de pouvoir identifier les incidents et leurs auteurs, afin de dissuader ces derniers et de mettre en place les mesures nécessaires à minimiser le risque numérique d'origine criminelle, ceux liés à des défauts de prise en compte adéquate des besoins de sécurité ou au détournement des technologies. Car, dès lors qu'il y a un sentiment d'impunité, qu'aucune limite convaincante existe, que la prise de risque est minimale et la profitabilité maximale, il y a des opportunités pour l'expression de la criminalité, mais aussi pour des usages abusifs pouvant émaner d'entités privées ou étatiques tout à fait licites.

Conclusion

Pouvoirs publics, législateurs, propriétaires et opérateurs d'infrastructures, utilisateurs, fournisseurs de solutions informatiques, il est du devoir de toutes les parties prenantes de contribuer à la sécurisation du cyberespace au bénéfice de la collectivité.

Il est vrai que cybersécurité et cyberdéfense sont quelquefois présentées comme un luxe pour les pays en voie de développement et ne font pas partie des priorités nationales qui se manifestent dans les constructions de dispensaires et d'hôpitaux, la formation du personnel de santé, les constructions de salles de classe, les créations d'emplois pour les jeunes, pour ne donner que quelques exemples. Se limiter à une telle vision reviendrait à oublier que derrière chacune de ces actions, il existe désormais un système d'information pour les soutenir. Or, c'est de la qualité, de la sécurité et de la valeur du système d'information qui sous-tend, par exemple, la stratégie nationale de la santé, qui pilote les programmes d'emplois des jeunes, ou encore de ceux mis en œuvre dans la gestion des finances publiques que dépend le fonctionnement de la société, de l'économie et de l'État. Au 21e siècle, nourrir les Hommes passe également par des systèmes d'information (culture, gestion des ressources, de l'accès à l'eau, à l'énergie, aux marchés, import/export, chaînes d'approvisionnement…). Qu'adviendrait-il de la santé ou des finances publiques, si leurs systèmes d'information traitent des données qui ne sont pas disponibles, intègres, « exactes » ou dignes de confiance ? Plusieurs pays ont vécu l'expérience malheureuse des listes électorales qui ne sont pas jugées dignes de confiance ; ce sont des exemples patents de manquement aux principes de cybersécurité, notamment à l'exactitude des données présentes dans le système, ce qui relève d'une problématique de sécurité informatique.

La cybersécurité et la cyberdéfense ne sont pas des luxes, elles jouent un rôle essentiel dans la capacité des pays à contribuer à leur développement économique et social et à leur reconnaissance internationale. Pour garantir leur sécurité et leur bien-être économique, tous les pays se doivent de renforcer leur posture de cybersécurité, de lutte contre la cybercriminalité et de cyberdéfense et de contribuer individuellement et collectivement aux processus de paix qui, désormais, passe également par la construction d'écosystèmes numériques de confiance et par la maîtrise des questions de sécurité et de défense dans le cyberespace.

Glossaire

Analyse de risque — Processus d'identification et d'évaluation des risques (estimation de leur probabilité d'occurrence et de leurs impacts).

Analyse des menaces — Processus d'identification des menaces potentielles contre des ressources qui, si elles se réalisent, leur portent atteinte.

Antivirus — Programme de détection de codes malveillants (de virus).

Architecture de sécurité — Ensemble des éléments matériels, logiciels, organisationnels et humains permettant de réaliser une politique de sécurité.

Authentification — Action d'authentifier. L'authentification sert à confirmer (ou non) qu'une action, déclaration, information est authentique (originale, vraie). Processus mis en œuvre, notamment, pour vérifier l'identité d'une entité et s'assurer que l'identité fournie correspond à l'identité de cette entité préalablement enregistrée. Fonction de sécurité contribuant à garantir la véracité d'une identité.

Blockchain — (Chaîne de blocs) — Application particulière des techniques de chiffrement pour développer des services de confiance distribuée.

Botnet (réseau de machine zombies) — mot construit à partir des mots robot et network faisant référence à un ensemble de systèmes infectés, pilotés et contrôlés à distance par un malveillant, pour réaliser des attaques (notamment en déni de service).

Cookies — Fichiers envoyés sur le poste de travail des internautes à leur insu, lors de l'accès à certains sites web, qui récoltent des informations les concernant pour en principe, la personnalisation des services web offerts.

Correctif de sécurité — Rustine de sécurité d'un logiciel pour en supprimer une vulnérabilité qui a été identifiée après son installation.

Cryptanalyse – La cryptanalyse comprend l'ensemble des moyens qui permet d'analyser une information préalablement chiffrée, afin de la déchiffrer. Plus un système de chiffrement est robuste, plus sa cryptanalyse est difficile.

Cryptographie — Application des mathématiques permettant d'écrire de l'information de manière à la rendre inintelligible à ceux ne possédant pas les capacités de la déchiffrer. Voir Chiffrement.

Cyberattaque — Attaque informatique réalisée à distance, via les technologies de l'Internet sur des systèmes connectés à Internet.

Cybercriminalité — Criminalité s'exprimant via les technologies de l'information et de l'Internet. L'ordinateur et le réseau sont des moyens et/ou des cibles de la criminalité.

Cyberdéfense — Concept de sécurité nationale et militaire d'un État qui tient compte du cyberespace, des technologies de l'information, des besoins de protection et de défense de ses infrastructures vitales et de l'évolution de la manière de faire la guerre, y compris par des moyens non militaires. La cyberdéfense englobe les concepts d'informatique offensive et défensive.

Cyberespace — Espace créé par l'humain, résultant de la mise en réseau des ordinateurs et de la dématérialisation de l'information et des activités.

Cyberpouvoir — Pouvoir conféré par la maîtrise du cyberespace et de la cybersécurité ou encore par la maîtrise des technologies de l'information et de la communication et de leurs vulnérabilités.

Cyberrésilience — Capacité à résister à des cyberattaques. État d'un environnement informatique connecté à Internet suffisamment robuste pour résister à des événements portant atteinte à sa sécurité et continuer à opérer.

Cybersécurité – Sécurité informatique et réseaux appliqués au cyberespace, aux activités et services en ligne et aux systèmes d'information ouverts sur l'Internet.

DDoS (Distributed Denial of Service) — Attaque par saturation (ou déni de service) lancée simultanément à partir de plusieurs systèmes.

Disponibilité — Critère de sécurité permettant que les ressources soient accessibles et utilisables selon les besoins (pas de refus d'accès autorisé aux systèmes, services, données, infrastructures, etc.).

Fraude – Utilisation non autorisée et détournement des ressources du système d'information, conduisant à un préjudice. Les vols des services sans fil, satellites, ou de lignes terrestres sont des exemples de fraude aux télécommunications. La fraude d'enchère, le non-paiement

ou la non-livraison des marchandises sont des exemples de fraude de confiance qui peuvent se réaliser au travers des services marchands d'Internet par exemple.

Gestion des risques – Processus continu d'évaluation des risques encourus par une organisation afin de les maîtriser, de les réduire à un niveau acceptable. Permet de déterminer la politique de sécurité la plus adaptée à la protection des valeurs de l'organisation.

Hacker — Action consistant à s'introduire de manière illicite dans un système. Un hackeur ou pirate informatique est une personne qui, quelle que soit sa motivation, pénètre sans autorisation et de manière illégale, dans un système appartenant à un tiers. Le piratage informatique (Hacking) est un ensemble des opérations conduisant généralement à une intrusion dans un système à des fins malveillantes (vol, détournement de capacité, destructions...).

Hameçonnage (Phishing) — Procédé de leurre des internautes pour les amener à réaliser certaines actions (consultation de sites web contrôlés par des malveillants…) ou à livrer des informations qu'ils n'auraient pas données s'ils n'avaient pas été abusés (informations confidentielles, personnelles…).

Ingénierie sociale — Techniques utilisées par des malveillants pour obtenir des informations auprès des personnes afin de leurrer des systèmes informatiques ou de contourner les mesures de sécurité. Capacité à exploiter les failles humaines, pour ensuite réaliser des cyberattaques, pouvant faire appel à la manipulation, l'intimidation, l'écoute, la surveillance de données, l'exploitation des données publiées sur des réseaux sociaux (open source intelligence), l'escroquerie, la crédulité ou de la naïveté des internautes, par exemple.

Intégrité — État d'une chose qui est demeurée intacte. Critère de sécurité, qui s'il est réalisé, permet de s'assurer qu'une ressource n'a pas été altérée (modifiée ou détruite) d'une façon non autorisée.

Intelligence économique — Capacité à maîtriser l'information stratégique (recherche, collecte, traitement) à des fins de performance et de compétitivité économiques.

Menace — Signe, indice qui laisse prévoir un danger. Action ou événement susceptible de se produire, de se transformer en agression contre un environnement et de porter préjudice à sa sécurité. Menaces délibérées (attaques), menaces involontaires (erreurs, défaillances, événements naturels, etc.), menaces connues, inconnues, etc., menace active (active threat), menace d'un changement délibéré et non autorisé de l'état du système (modification d'un message, génération de faux messages, déni de service, etc.) ; menace passive (passive threat), menace d'une divulgation d'information confidentielle, sans modification de l'état du système.

Mesures de sécurité — Ensemble de moyens technologiques, organisationnels, juridiques, financiers, humains, procéduraux et d'actions permettant d'atteindre les objectifs de sécurité

fixés par le politique de sécurité. Les mesures sont généralement classifiées selon leur rôle fonctionnel (ex. : mesure de prévention, de protection, de dissuasion, etc.).

Plan de gestion de crise — Ensemble des moyens techniques et organisationnels prévus pour répondre optimalement à un incident grave affectant la bonne marche des opérations et préjudiciable à l'organisation.

Plan de secours — Ensemble des moyens techniques et organisationnels prévus pour assurer la pérennité des informations et la continuité des activités, quels que soient les problèmes rencontrés.

Politique de sécurité — Référentiel de sécurité établi par une organisation, reflétant sa stratégie de sécurité et spécifiant les moyens de la réaliser.

Porte dérobée (backdoor, trap door) — Fait le plus souvent référence à un morceau de code intégré dans des logiciels permettant l'accès dissimulé, la prise de contrôle d'un système, la copie d'information, etc. à l'insu de son propriétaire.

Protection des données privées et de l'intimité numérique (privacy protection) – Mesures de protection qui permettent d'assurer que les informations, les activités des internautes, ne soient pas révélées à d'autres parties que celles voulues et ne soient pas utilisées à des fins contraires à celles consenties par leur propriétaire. Cela fait référence au droit des individus de contrôler les informations les concernant qui peuvent être collectées soit directement, soit indirectement par observation de leur comportement de navigation et sites visités.

Rançongiciel (ransomware) — Logiciel malveillant prenant le contrôle des ressources d'un internaute afin de les lui rendre indisponibles pour exercer un chantage et exiger le paiement d'une rançon.

Risque (risk) – Danger plus ou moins probable émanent d'une menace et pouvant se traduire en termes de probabilité d'apparition et de niveau d'impact.

Sécurité – Situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger. Mécanisme destiné à prévenir un événement dommageable, ou à en limiter les effets. Par exemple, la sécurité physique (physical security) est relative aux mesures permettant d'offrir une protection physique, matérielle des environnements, tandis que la sécurité logique (logical security) fait référence aux procédures et moyens logiciels de protection.

Sécurité de l'information — Ensemble de mesures techniques et non techniques visant à assurer la disponibilité, l'intégrité ou la confidentialité des données.

Spamming — Technique qui consiste à envoyer des messages électroniques non sollicités.

Usurpation d'identité (identity theft) — Emprunt de l'identité de personnes réelles pour obtenir frauduleusement des prestations en leur nom et place ou pour réaliser des actions délictueuses et leur faire porter la responsabilité de celles-ci.

Virus — Programme malveillant introduit, à l'insu des utilisateurs, dans un système. Il possède la capacité de se dupliquer — soit à l'identique, soit en se modifiant (virus polymorphe) —, de porter atteinte aux environnements dans lequel il s'exécute, et de contaminer les autres utilisateurs avec lesquels il est en relation. Différents types de virus sont distingués en fonction de leur signature, de leur comportement, de leur type de reproduction, de l'infection, des dysfonctionnements induits, etc. Les vers, chevaux de Troie, bombes logiques sont des codes malveillants de la famille générique des virus.

Vulnérabilité (vulnerability) — Défaut de sécurité qui pourrait se traduire, soit intentionnellement, soit accidentellement par une violation de la politique de sécurité.

Zéro-day (jour 0) — Qualifie les vulnérabilités qui n'ont pas encore fait l'objet de contre-mesure de sécurité ou de correctif et qui peuvent être exploitées pour réaliser des attaques informatiques.

Document produit par la Direction de la Francophonie économique et numérique
(sous la coordination d'Emmanuel Adjovi, spécialiste de programme « société de l'information ») et
réalisé par la Direction de la communication et des instances de la Francophonie.

ISBN : 978-92-9028-429-1

L'Organisation internationale de la Francophonie (OIF) est une institution fondée sur le partage d'une langue, le français, et de valeurs communes. Elle rassemble à ce jour 84 États et gouvernements, dont 58 membres et 26 observateurs. Le Rapport sur la langue française dans le monde 2014 établit à 274 millions le nombre de locuteurs de français.

Présente sur les cinq continents, l'OIF mène des actions politiques et de coopération dans les domaines prioritaires suivants : la langue française et la diversité culturelle et linguistique ; la paix, la démocratie et les droits de l'Homme ; l'éducation et la formation ; le développement durable et la solidarité. Dans l'ensemble de ses actions, l'OIF accorde une attention particulière aux jeunes et aux femmes ainsi qu'à l'accès aux technologies de l'information et de la communication.

Elle s'attache à développer le multilinguisme comme facteur indispensable de communication harmonieuse entre les peuples et à sensibiliser à l'importance de la promotion de la diversité linguistique comme composante essentielle de la diversité culturelle.

58 États et gouvernements membres et associés

Albanie • Principauté d'Andorre • Arménie • Royaume de Belgique • Bénin • Bulgarie • Burkina Faso • Burundi • Cabo Verde • Cambodge • Cameroun • Canada • Canada–Nouveau-Brunswick • Canada-Québec • République centrafricaine • Chypre • Comores • Congo • République démocratique du Congo • Côte d'Ivoire • Djibouti • Dominique • Égypte • Ex-République yougoslave de Macédoine • France • Gabon • Ghana • Grèce • Guinée • Guinée-Bissau • Guinée équatoriale • Haïti • Laos • Liban • Luxembourg • Madagascar • Mali • Maroc • Maurice • Mauritanie • Moldavie • Principauté de Monaco • Niger • Nouvelle-Calédonie • Qatar • Roumanie • Rwanda • Sainte-Lucie • Sao Tomé-et-Principe • Sénégal • Seychelles • Suisse • Tchad • Togo • Tunisie • Vanuatu • Vietnam • Fédération Wallonie-Bruxelles

26 observateurs

Argentine • Autriche • Bosnie-Herzégovine • Canada-Ontario • Costa Rica • Croatie • République de Corée • République dominicaine • Émirats arabes unis • Estonie • Géorgie • Hongrie • Kosovo • Lettonie • Lituanie • Mexique • Monténégro • Mozambique • Pologne • Serbie • Slovaquie • Slovénie • République tchèque • Thaïlande • Ukraine • Uruguay

ORGANISATION INTERNATIONALE DE LA FRANCOPHONIE
19-21, avenue Bosquet, 75007 Paris — France
Tél. : +33 (0)1 44 37 33 00
francophonie.org
OIFfrancophonie

ORGANISATION INTERNATIONALE DE
la francophonie