futuribles
INTERNATIONAL

Entreprises et cybersécurité

Étude en souscription 2013

ASSOCIATION FUTURIBLES INTERNATIONAL
47, rue de Babylone - 75007 Paris - France - Tél. 33 (0)1 53 63 37 70 - Fax 33 (0)1 42 22 65 54
E-mail forum@futuribles.com - Site Internet www.futuribles.com

Les risques cyber évoluent vite, obligeant les entreprises et les administrations publiques à réagir sur des temps très courts. Cette urgence permanente peut prendre le pas sur les réflexions sur les évolutions des risques à moyen et long termes, et sur les stratégies qui pourraient permettre de les réduire.

Considérant qu'une réflexion à moyen terme sur les questions de cybersécurité peut être porteuse d'enseignements utiles à la mise en place de stratégies de réduction des risques à différentes échelles (États, entreprises, individus), considérant qu'une approche mutualisée peut être bénéfique à la réflexion des acteurs concernés, Futuribles International lance une étude intitulée « Entreprises et cybersécurité ».

L'étude s'appuiera sur la méthode des scénarios pour mettre en évidence les enjeux majeurs de la cybersécurité de demain, et ainsi permettre l'élaboration de stratégies à moyen et long termes en matière de cybersécurité pour les entreprises. Cette analyse prospective amènera à prendre une nécessaire distance par rapport aux évolutions incessantes et à réfléchir aux articulations des différentes temporalités à l'œuvre dans le domaine de la cybersécurité : temps long des développements d'outils de gestion et de production des entreprises, et temps court de l'évolution des modes d'attaques ; temps long de la réponse judiciaire ou politique à l'attaque par rapport au temps court de la gestion technique et opérationnelle de crise pour permettre la continuité de l'activité de l'entreprise. La fonction de veille et d'anticipation assurée par cette étude paraît indispensable pour développer et maintenir des systèmes d'information performants et sécurisés, car intégrant en amont les risques de demain.

Les organismes qui participent à cette étude contribuent à sa réalisation. Ils en constituent le comité d'orientation, régulièrement réuni et consulté, et en assurent le financement.

CONFIDENTIALITÉ

Futuribles travaillera en étroite collaboration avec les organismes **ayant souscrit** à cette étude. Les données qui pourraient être transmises dans le cadre de cette étude seront traitées avec la plus grande confidentialité. Trois niveaux de confidentialité seront distingués : les informations données à titre confidentiel aux directeurs de l'étude et non réutilisables telles quelles dans les livrables ; les informations pouvant être mutualisées au sein des organismes participant à l'étude ; les informations pouvant éventuellement être rendues publiques.

S'il était décidé par les organismes participant à l'étude de produire un rapport public, celui-ci ne pourrait être publié qu'après leur accord. L'association se réserve par ailleurs le droit de ne pas donner suite à la demande de participation à cette étude d'une entreprise dont les activités laisseraient penser qu'elle ne partage pas nécessairement les objectifs présentés dans ce document. La confiance mutuelle entre organismes participant à cette étude est une condition essentielle de sa réussite.

Exposé des motifs

Le cyberespace au centre des activités des entreprises

Par cyberespace on entend l'ensemble des données numérisées constituant un univers d'information et de communication. Le cyberespace est le lieu par lequel transitent des données cruciales à l'activité des entreprises, aussi bien dans leurs relations internes (ressources humaines, recherche-développement, gestion financière, management...) que dans leurs relations externes (clients, sous-traitants, fournisseurs...) Le cyberespace est un lieu de travail, de transaction financière, d'archivage, etc.

La cybersécurité, un enjeu stratégique

La stratégie de sécurité est une condition nécessaire pour tirer un profit positif du cyberespace. La cybersécurité vise en effet à garantir la disponibilité et l'intégrité du cyberespace, et la confidentialité des données qui y transitent. La cybersécurité est stratégique pour l'entreprise car elle participe, comme l'illustre le tableau 1 (ci-contre), à la sécurité économique, à la compétitivité des entreprises, à la résilience des organisations, et à la limitation de dommages matériels et immatériels pouvant toucher aux actifs des firmes via le cyberespace, dans un monde où les entreprises sont en réseau(x).

Partant de ces constats, Futuribles international se propose de mener une étude prospective qui puisse contribuer à replacer les enjeux de cybersécurité dans une perspective systémique et stratégique de moyen et long termes pour les entreprises françaises.

Tableau 1 — Cinq enjeux stratégiques de la cybersécurité pour les entreprises	
Cybersécurité et sécurité économique	La sécurité économique vise à protéger les informations stratégiques confiées aux entreprises par l'État. Les exemples sont nombreux où l'État s'appuie sur des opérateurs pour gérer des infrastructures dites « critiques », car vitales pour le bon fonctionnement du pays. Parmi les infrastructures critiques figurent par exemple les réseaux de communication, les réseaux de transport, les réseaux de production et d'approvisionnement énergétiques, etc. Si ces opérateurs privés font l'objet d'attaques cyber, cela met en péril, au-delà des entreprises, le bon fonctionnement de l'État et de la société. La cybersécurité constitue donc bien, pour ces acteurs privés et pour l'État, un enjeu stratégique.
Cybersécurité et compétitivité des entreprises	Les entreprises, pour rester compétitives, ont besoin de préserver leurs avantages concurrentiels ; cela repose sur la protection des brevets, des données scientifiques et techniques de pointe, des données financières confidentielles, un projet *marketing* innovant, etc. Ce capital intellectuel est crucial pour rester compétitif sur des marchés très concurrentiels. Or, de plus en plus, l'usage du *cloud*, la multiplication de supports mobiles de travail (*smartphones*, tablettes) rendent l'accès à ces données stratégiques non seulement possible mais aussi facilité en créant de nouvelles failles. Savoir identifier les données à protéger en priorité et s'armer pour défendre leur accès est donc stratégique pour les entreprises et leur compétitivité.
Cybersécurité et résilience des entreprises	La cybersécurité touche de près à la résilience des entreprises. Par exemple, elle concerne la capacité à maintenir une continuité des activités, même si des pannes de réseaux ou des attaques volontaires survenaient. Or, sans accès au cyberespace, les entreprises sont aujourd'hui le plus souvent bloquées dans leurs opérations du quotidien (échange de courriers électroniques, transactions, suivi des commandes, etc.).
Cybersécurité et limitation des dommages matériels et immatériels touchant aux actifs de l'entreprise	Les attaques cyber ont un coût financier pour l'entreprise quand, par exemple, il faut racheter du matériel neuf. Les attaques cyber peuvent aussi avoir un coût immatériel en nuisant à l'image de marque de l'entreprise car elles soulignent les failles d'un système de production, d'exploitation. Un exemple typique de dommage immatériel est celui de la perte ou du vol de données confiées à l'entreprise par des tiers (clients, fournisseurs). Cela atteint la crédibilité de l'entreprise, la confiance que peuvent lui témoigner ses clients, etc. La cybersécurité est donc importante pour limiter les dommages matériels et immatériels touchant les actifs clefs de l'entreprise.
Cybersécurité et entreprise en réseau(x)	Les entreprises sont aujourd'hui des entités poreuses, car connectées à de nombreux acteurs par les systèmes d'information. Si le degré de connexion peut faire la force des grands groupes, cela peut aussi être une faiblesse lorsqu'il s'agit de garantir la sécurisation des données. Il n'est plus possible de penser l'entreprise comme une forteresse, et il reste à la concevoir comme un réseau résilient à travers une stratégie systémique de cybersécurité.

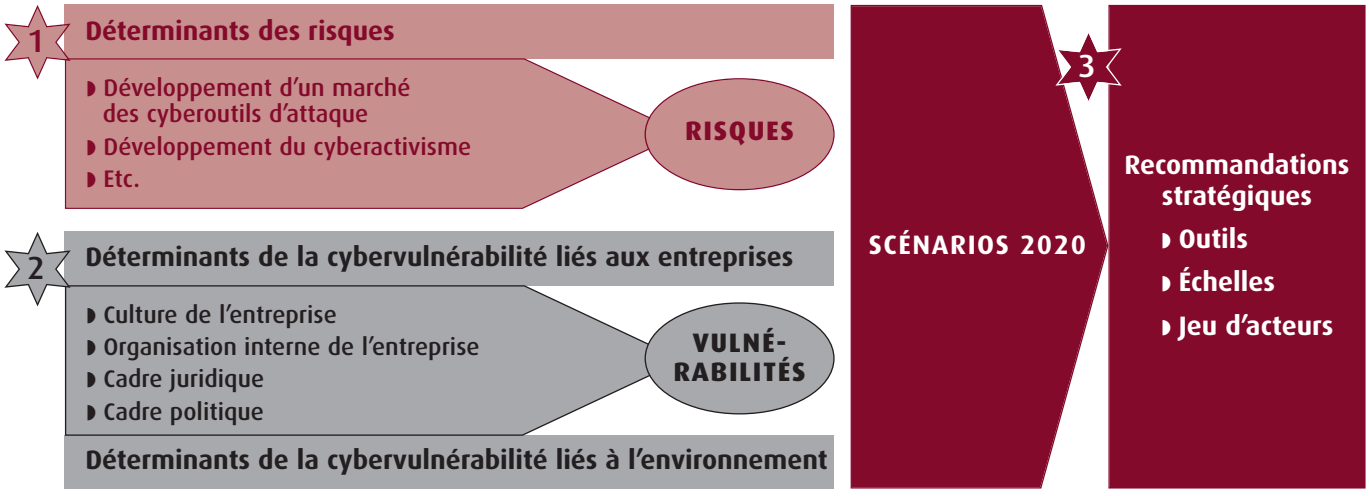
Périmètre

L'étude s'attachera à envisager les enjeux de la cybersécurité relevant autant de la **protection des systèmes et des logiciels**, que de la **protection des informations stockées** via ces supports.

Au-delà des documents publics qui seront analysés dans le cadre de ce travail, des études de cas plus détaillées seront conduites, principalement au sein des entreprises participant à l'étude sur la base d'entretiens avec les personnes concernées.

Objectifs de l'étude

L'objectif de l'étude est d'identifier quels seront les enjeux stratégiques en termes de cybersécurité pour les entreprises à l'horizon 2020. Futuribles propose de mener la réflexion en trois temps : identification des déterminants des risques, identification des déterminants de la cybervulnérabilité liés à l'organisation et à son environnement, construction de scénarios à des fins de recommandations stratégiques.



1. Typologie rétrospective et prospective des risques

Cette première phase consistera à **identifier les déterminants majeurs des menaces** (par types d'acteurs, intentions, capacités) **et, plus largement, des risques** tels que les pannes techniques, les pertes de matériel par oubli (exemples : oubli d'un téléphone portable, perte d'un ordinateur portable), les catastrophes naturelles, etc. Les déterminants qui seront étudiés pourront inclure des phénomènes nouveaux, non encore perçus aujourd'hui comme risques, mais qui pourraient le devenir.

Ce diagnostic sera mis en discussion lors d'une réunion de travail d'une journée du comité d'orientation. Une liste de 5 à 10 grands déterminants des risques cyber sera alors retenue.

Futuribles analysera, pour chacun des déterminants, son évolution rétrospective sur les 10 dernières années, et prospective à l'horizon 2020, sur la base d'études documentaires et d'études de cas d'entreprises parmi les organisations participant à l'étude (réalisation d'entretiens).

Cela donnera lieu à l'élaboration d'**une fiche par déterminant.** Les fiches seront présentées dans le premier rapport remis aux participants.

2. Une analyse rétrospective et prospective des déterminants de la vulnérabilité des entreprises

L'objectif de cette deuxième phase sera de **cerner les déterminants de la vulnérabilité cyber des entreprises,** que ces déterminants soient **liés à l'organisation elle-même** (niveau micro) **ou à son environnement** (niveau macro).

Par cybervulnérabilité on entend d'une part l'ensemble des **fragilités** de l'entreprise et de son environnement (par exemple, le facteur humain avec des employés peu formés aux risques cyber), et d'autre part **l'ensemble des éléments de l'entreprise ou de son environnement qui pourraient ou non l'aider à faire face aux risques, à s'adapter, à répondre** (par exemple, assurance contre les risques cyber). La vulnérabilité a donc deux facettes : les failles pouvant faciliter les attaques, mais aussi la capacité d'adaptation et de réponse face aux risques.

Des données en source ouverte seront collectées et analysées par Futuribles international, ainsi que les renseignements fournis par les organisations participant à l'étude. Des études de cas en France et à l'étranger seront conduites auprès de différentes organisations sur la base d'entretiens avec les services concernés.

Une liste de déterminants de la cybervulnérabilité sera alors soumise aux organisations participant à l'étude. À titre d'exemple, le tableau 2 ci-dessous présente des déterminants envisageables.

Tableau 2 — Exemples de déterminants de la cybervulnérabilité

Déterminants liés à l'entreprise (niveau micro)	Déterminants liés à l'environnement de l'entreprise (niveau macro)
◗ Déterminants architecturaux (connexion ou déconnexion des systèmes, accès restreint ou ouvert aux réseaux, complexité du système d'information, couplage ou découplage Internet / Intranet, *cloud* ou non, etc.)	◗ Déterminants politiques (politique de sécurité numérique, priorité donnée à la cybersécurité par rapport à d'autres risques, investissement public dans la cybersécurité, etc.)
◗ Déterminants organisationnels (taille de l'entreprise, place de la cybersécurité dans l'organigramme, date de l'émergence de la cybersécurité comme fonction dans l'entreprise, etc.)	◗ Déterminants normatifs / réglementaires (harmonisation des normes, certification du matériel, etc.)
◗ Déterminants interorganisationnels (interconnexion avec les prestataires, clients, etc.)	◗ Déterminants juridiques / légaux (droit relatif à la protection des données, droit relatif à la protection du secret, modes de répression judiciaire, etc.)
◗ Déterminants financiers (chiffre d'affaires de l'entreprise, investissement dans les systèmes de sécurité des informations)	◗ Déterminants économiques (ex. : diversification des activités des groupes avec multiplication des champs d'activités et donc des systèmes d'information)
◗ Déterminants liés à la culture d'organisation (BYOD*, télétravail, règlements internes sur l'usage des systèmes d'information, formations à la cybersécurité, etc.)	◗ Déterminants sociaux (ex. : usage des réseaux sociaux, brouillage de la frontière sphère privée / sphère publique, etc.)
◗ Déterminants liés au profil des recrutés (jeunes / âgés, familiers ou non des questions informatiques, à comportement à risques ou non, etc.)	◗ Déterminants géostratégiques (ex. : internationalisation des entreprises, existence de « paradis numériques »)
◗ Déterminants liés au lien avec les services de l'État (Agence nationale de la sécurité des systèmes d'information, ministère de la Défense, etc.)	◗ Déterminants assurantiels (évolution du marché de la cyberassurance)
**Bring Your Own Device* (fait d'amener son matériel personnel).	

Une journée de réunion de travail du comité d'orientation sera organisée pour valider une quinzaine de déterminants clefs de la cybervulnérabilité. **Futuribles analysera l'évolution rétrospective et prospective** de ces déterminants pour produire des fiches sur chacun d'eux. L'ensemble de ces fiches fera l'objet du deuxième rapport.

3. Élaboration de scénarios stratégiques de modes de gouvernance efficace de la cybersécurité de l'entreprise en 2020

L'objectif de cette troisième phase sera de développer des scénarios relatifs au mode de gouvernance de la cybersécurité des entreprises en 2020. La vocation des scénarios est de mettre en évidence les **enjeux stratégiques clefs**.

Pour cela, on utilisera la méthode des scénarios. Il s'agira donc de construire des scénarios intermédiaires (microscénarios) sur les risques, d'une part, et sur la cybervulnérabilité, d'autre part, en s'appuyant sur les analyses rétrospectives et prospectives des déterminants effectuées lors des phases précédentes. Il s'agira ensuite d'articuler ces microscénarios entre eux pour construire des scénarios globaux. Ces microscénarios et scénarios globaux seront élaborés collectivement lors de journées de travail qui seront proposées aux organisations participant à l'étude et à des experts du sujet.

Les scénarios donneront lieu à des recommandations stratégiques en soulignant trois aspects :

- **Les outils.** Évaluation des outils de gouvernance de la cybersécurité et de leur pertinence : certification, labels, guide de bonnes pratiques, formation, centre de gestion des cyberattaques, cercle de confiance d'entreprises, assurances, dispositifs d'alerte intrusion, isolement des éléments clefs de l'entreprise, etc.
- **Les échelles.** Évaluation des différents niveaux de gouvernance et de leur pertinence : international, Europe, France, entreprise, levier des individus, pour cerner ce qui doit être du ressort de l'entreprise mais aussi ce qui doit passer par des changements au niveau des autres échelles d'action possibles.
- **Le jeu d'acteurs.** Évaluation des modes de conjugaison des efforts : les partenariats public-privé, l'intégration verticale (de l'État à l'individu en passant par l'entreprise), l'intégration horizontale (entre entreprises).

Les scénarios et recommandations feront l'objet du rapport final. **Cette étude sera conduite par des experts de haut niveau et en étroite intelligence avec les organismes y ayant souscrit qui seront réunis à chacune des étapes de la démarche.**

Les produits de la démarche

- Une note de diagnostic et de problématique pour stabiliser avec les participants le périmètre de l'étude.
- Un rapport présentant 5 à 10 déterminants clefs des risques cyber pour les entreprises françaises sur la base :
  - d'une analyse documentaire à partir de sources ouvertes et d'informations fournies par les organismes participants ;
  - d'entretiens avec des experts et avec les personnes concernées au sein des organismes participant à l'étude (services en charge des systèmes d'information, de la sécurité, etc.) ;
  - d'une journée de travail avec le comité d'orientation, afin d'avoir une approche commune et systémique des risques, et de retenir 5 à 10 déterminants clefs ;
  - de la rédaction de fiches documentant les déterminants identifiés de façon rétrospective et prospective.
- Un rapport présentant une quinzaine de déterminants clefs de la cybervulnérabilité en entreprise sur la base :
  - d'une analyse documentaire sur sources ouvertes et d'informations communiquées par les organismes participants ;
  - d'entretiens avec des experts et avec les personnes concernées au sein des organisations participantes ;
  - d'une journée de travail avec le comité d'orientation, permettant de retenir 15 déterminants clefs ;
  - de la rédaction de fiches documentant les déterminants identifiés de façon rétrospective et prospective.

◗ **Un rapport présentant différents scénarios contrastés de modes de gouvernance efficaces de la cybersécurité pour les entreprises en 2020 et des recommandations stratégiques sur la base :**

- de deux jours de travail d'élaboration des scénarios avec le comité d'orientation ;
- de recommandations stratégiques en termes d'outils, d'échelles d'intervention et de jeux d'acteurs appropriés.

◗ Une synthèse courte de l'étude sous forme de diaporama commenté qui puisse être aisément utilisé dans des présentations au sein des organismes participant à l'étude.

À l'issue de l'étude, on envisagera l'opportunité d'organiser une conférence de valorisation de ces travaux.

Pilotage, équipe de réalisation et contact

Directeurs d'étude : **Cécile Wendling,** Futuribles International, et **Nicolas Mazzucchi,** expert extérieur

Chargée d'étude : **Laurie Grzesiak,** Futuribles International

Conseiller scientifique de l'étude : **Olivier Kempf,** maître de conférences à Sciences Po Paris, directeur de la collection de cyberstratégie chez Economica

Comité scientifique (en cours de constitution) :

- **Bertrand Collomb,** président d'honneur du groupe Lafarge et membre de l'Institut.
- **Geoffrey Delcroix,** chargé d'études Innovation et prospective, CNIL (Commission nationale de l'informatique et des libertés).
- **Frederick Douzet,** titulaire de la chaire Castex de cyberstratégie à l'Institut des hautes études de défense nationale, et directrice adjointe de l'Institut français de géopolitique, université Paris 8.
- Lieutenant-colonel **Rémy Février,** chargé de mission Intelligence économique et Sécurité des systèmes d'information, Gendarmerie nationale ; professeur associé à l'université Paris I-Sorbonne.
- **Françoise Gri,** directrice générale du groupe Pierre & Vacances-Center Parcs.
- **Bruno Gruselle,** chercheur à la Fondation pour la recherche stratégique.
- **François Bernard Huygues,** directeur de recherche à l'Institut de relations internationales et stratégiques (IRIS), spécialisé sur la communication, la cyberstratégie et l'intelligence économique.
- **Myriam Quemener,** magistrate et auteur de nombreux ouvrages sur la cybercriminalité
- **Daniel Ventre,** titulaire de la chaire de cyberdéfense et cybersécurité Saint-Cyr / Sogeti / Thales Communications & Security.
- Général d'armée (2S) **Marc Watin-Angouard,** directeur du centre de recherche de l'école des officiers de la Gendarmerie nationale et délégué au Forum international de la cybersécurité (FIC).

Comité d'orientation (en cours de constitution) : composé des représentants des organisations participant à l'étude, il se réunit aux étapes clefs de l'étude. Ses membres sont les principaux destinataires des documents fournis. Ils sont les interlocuteurs de l'équipe de réalisation du projet. Les organisations participantes peuvent désigner deux personnes pour les représenter dans le comité d'orientation de l'étude.

Contact : **Cécile Wendling** - tél. + 33 (0)1 53 63 37 79 - cwendling@futuribles.com

Calendrier

Phase 1. Septembre-décembre 2013

◗ Réunion de lancement

◗ Élaboration d'une liste des déterminants des cyberrisques.

◗ Une journée de réunion de travail du comité d'orientation pour retenir les déterminants clefs qui donneront lieu à l'élaboration de fiches variables.

◗ Analyse documentaire et entretiens pour compléter les fiches variables qui feront l'objet du premier rapport.

Phase 2. Janvier-avril 2014

◗ Identification de déterminants de la cybervulnérabilité des entreprises.

◗ Réunion de travail d'une journée du comité d'orientation pour retenir les 15 variables déterminantes de la cybervulnérabilité.

◗ Analyse documentaire et entretiens pour compléter les fiches variables qui feront l'objet du deuxième rapport.

Phase 3. Mai-août 2014

◗ Deux jours de réunion de travail du comité d'orientation pour construire les trames de scénarios.

◗ Élaboration des microscénarios sur les risques, et sur la cybervulnérabilité.

◗ Élaboration des scénarios globaux de gouvernance de la cybersécurité pour les entreprises.

◗ Réunion du comité d'orientation : restitution des scénarios et élaboration des recommandations.

◗ Rapport final de synthèse qui inclura des recommandations, en fonction des types d'entreprises concernées et des échelles d'action.

ENTREPRISES ET CYBERSÉCURITÉ

MODALITÉS ET BULLETIN DE SOUSCRIPTION

À retourner à Futuribles International - 47, rue de Babylone - 75007 Paris - France
Tél. + 33 (0)1 53 63 37 70 - Fax + 33 (0)1 42 22 65 54 - e-mail forum@futuribles.com - Site Internet www.futuribles.com
N° TVA : FR 21.784314940 - N° SIRET : 784 314 940 00056

La souscription à cette étude est ouverte à partir de mars 2013. Les travaux commenceront dès que le nombre minimum de souscripteurs sera atteint. Le prix de la souscription est de 15 000 euros hors taxes soit 17 940 euros TTC (dont TVA à 19,6 % soit 2 940 euros), payables suivant l'échéancier suivant :

- 30 % (4 500 euros HT, soit 5 382 euros TTC dont TVA à 19,6 % de 882 euros) en fin de phase 1 ;
- 40 % (6 000 euros HT, soit 7 176 euros TTC dont TVA à 19,6 % de 1 176 euros) en fin de phase 2 ;
- 30 % (4 500 euros HT, soit 5 382 euros TTC dont TVA à 19,6 % de 882 euros) à l'achèvement des travaux.

Les membres partenaires de l'association Futuribles International bénéficient sur ce tarif d'une remise de 25 % et les membres associés d'une remise de 10 %.

Nom .....
Prénom .....
Fonction .....
Organisation .....
Adresse .....
.....
..... Code postal .....
Ville ..... Pays .....
Tél. ..... Fax .....
E-mail .....
N° TVA .....

❒ Membre partenaire de Futuribles International

Souscrit à l'étude « Entreprises et cybersécurité » pour un montant total de 11 250 euros HT, soit 13 455 euros TTC (dont TVA à 19,6 % = 2 205 euros), payable selon l'échéancier ci-dessus.

❒ Membre associé de Futuribles International

Souscrit à l'étude « Entreprises et cybersécurité » pour un montant total de 13 500 euros HT, soit 16 146 euros TTC (dont TVA à 19,6 % = 2 646 euros), payable selon l'échéancier ci-dessus.

❒ Non-membre de Futuribles International

Souscrit à l'étude « Entreprises et cybersécurité » pour un montant total de 15 000 euros HT, soit 17 940 euros TTC (dont TVA à 19,6 % = 2 940 euros), payable selon l'échéancier ci-dessus.

Correspondant principal

Nom .....
Prénom .....
Fonction .....
Service .....
Tél. ..... Fax .....
E-mail .....

Règlement :

❒ par chèque bancaire ou postal
à l'ordre de Futuribles International

❒ par virement bancaire : Banque Neuflize OBC,
3, avenue Hoche - F-75008 Paris
Code banque 30788, code guichet 00107
N° de compte 10202041200 clé 24
IBAN FR76 3078 8001 0710 2020 4120 024
BIC NSMBFRPPXXX

❒ par carte ❍ Visa ou ❍ American Express
N° ..... Expire .....
Cryptogramme figurant sur votre carte .....

❒ au reçu d'une facture

et s'engage à verser les sommes dues selon l'échéancier indiqué.

Fait à ....., le .....

Signature et cachet de l'organisation

futuribles INTERNATIONAL

47, rue de Babylone - 75007 Paris - France
N° TVA : FR 21.784314940 - N° SIRET 784 314 940 00056
Tél. 33 (0)1 53 63 37 70 - Fax 33 (0)1 42 22 65 54
E-mail forum@futuribles.com
Site Internet www.futuribles.com

ASSOCIATION FUTURIBLES INTERNATIONAL

47, rue de Babylone, 75007 Paris, France
Tél. + 33 (0)1 53 63 37 70 - Fax. + 33 (0)1 42 22 65 54
E-mail : forum@futuribles.com - Site Internet : www.futuribles.com

Explorer ce qui peut advenir
(les futurs possibles)
et ce qui peut être fait
(les politiques et les stratégies)

UNE ASSOCIATION INTERNATIONALE DE PROSPECTIVE, FUTURIBLES INTERNATIONAL...

✓ Veille

- Sur qui fait quoi, où et comment, dans le domaine des études prospectives
- Vigie : système de veille prospective sur l'environnement stratégique des entreprises et des organisations

✓ Forum prospectif

Plate-forme de rencontres entre experts et décideurs, Futuribles International organise des tables rondes, des journées d'étude et des colloques internationaux

✓ Formation

- Des sessions de formation aux concepts et aux méthodes de prospective
- Des sessions de formation à la prospective appliquée

✓ Études et recherche

Des études en souscription sont lancées sur différentes problématiques économiques, sociales, environnementales, etc.

...EN LIEN AVEC UNE SOCIÉTÉ DE PRESSE ET DE COMMUNICATION

✓ *Futuribles*, revue mensuelle pluridisciplinaire et prospective sur les grands enjeux du monde contemporain et ses évolutions possibles

✓ Une action permanente de sensibilisation aux futurs possibles au travers des médias (édition, production audiovisuelle...)

...ET UN PÔLE D'EXPERTISE EN PROSPECTIVE ET STRATÉGIE

✓ Des études de prospective appliquée

✓ Une activité de conseil en veille, prospective et stratégie auprès des entreprises et organismes publics