République Française

OFFICE PARLEMENTAIRE D'ÉVALUATION
DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES

Sécurité numérique et risques : enjeux et chances pour les entreprises

Rapporteurs : Mme Anne-Yvonne Le Dain, députée, et M. Bruno Sido, sénateur.

À l'heure de l'omniprésence du numérique et du développement constant de ses spectaculaires potentialités, ***les entreprises doivent pouvoir compter sur des outils numériques sécurisés****. Or, chaque jour, de tous côtés, les exemples de nouvelles vulnérabilités se multiplient.*

L'escalade entre les failles découvertes et les parades pour y remédier semble sans fin, d'autant plus que ***l'origine de ces fragilités réside dans nombre de comportements humains irréfléchis*** *et dans la lenteur de l'indispensable prise de conscience.*

Après avoir entendu plus d'une centaine de personnes et analysé en détail les atouts et les fragilités des messages numériques et de leurs canaux de diffusion, l'Office parlementaire d'évaluation des choix scientifiques et technologiques propose d'abord ***une trentaine de recommandations d'ordre général*** *(culture du numérique, souveraineté, coopération entre les acteurs, droit européen de la donnée)* ***puis un*** **vade-mecum** ***de sécurité numérique à l'usage des entreprises*** *qui voudront bien s'attacher à la construction réfléchie et évolutive dont dépend leur future prospérité.*

Face à la mondialisation numérique, l'élaboration de solutions se révèle être d'abord individuelle et nationale pour éviter que les entreprises françaises acquiescent elles-mêmes au pillage de leurs données en les offrant en libre-service.

I. LE CONTEXTE INTERNATIONAL DE LA SÉCURITÉ NUMÉRIQUE DES ENTREPRISES

A. La gouvernance technique du numérique à l'échelle mondiale

La toile d'araignée qui enserre le monde, le *Net*, l'*Internet*, le *web*, est en contact avec tous les secteurs d'activité. Les règles discrètes de sa mise en place et de son organisation ont bénéficié à des sociétés commerciales et à leur État d'origine tandis que la population mondiale se prêtait avec ardeur et inconscience à cette mainmise mondiale sur les esprits comme sur les objets.

L'organisation de la gouvernance de l'Internet (répartition des adresses *IP*, des noms des domaines *DNS* et d'autres éléments de fonctionnement du protocole Internet) **ne résulte d'aucun texte international**.

En 2014, à São Paulo, **l'Union européenne a prôné un Internet unique, ouvert, libre, sûr, fiable et non fragmenté**.

Mais **là où le droit devrait énoncer les règles, prévalent des rapports de force entre les géants de l'Internet, les États, les entreprises et les citoyens.**

B. La gestion mondiale des incidents de sécurité numérique

Rattaché au département nord-américain du commerce, le *National Institute of Standards and Technology (NIST)*, chargé de **favoriser la compétitivité des entreprises face à l'usage de technologies complexes,** a étendu son périmètre à la **normalisation des technologies de l'information**.

Le *NIST*, qui héberge et gère la base de connaissance des vulnérabilités au niveau national (*National Vulnerability Database*), est à l'origine de l'emploi ou du développement de la plupart des normes à des fins de veille en sécurité (bulletins *OVAL*, *CVE*, *CVSS*).

La connaissance de la majorité des vulnérabilités est concentrée sur le *Security Content Automation Protocol (SCAP)*, plate-forme du *NIST* assurant la mise en réseau de connaissances de sécurité entre la recherche scientifique et industrielle. **Le *SCAP* centralise et diffuse les événements de sécurité considérés comme dangereux afin de favoriser la coopération au niveau national et international.**

L'État nord-américain s'est également doté d'un centre de traitement des incidents informatiques, le *CERT/CC (Computer Emergency Response Team Coordination Center)*. **Le *CERT/CC* diffuse ces vulnérabilités au grand public dans des bulletins (*bugtraq*), mettant *de facto* les éditeurs de logiciels en demeure de corriger leurs failles. Le *CERT/CC* publie gratuitement au quotidien une liste des vulnérabilités et leur analyse détaillée.**

Le *CERT/CC* a développé un réseau à l'échelle mondiale pour fédérer les connaissances de sécurité scientifiques et industrielles et **offrir un service aux**

usagers du monde entier. **Chaque État ou entité demandant à rallier ce réseau doit être certifié par le *CERT/CC*.**
En France, il existe une vingtaine de *CERT* dont, certains *CERT* d'État, comme l'ANSSI.
L'émergence de ces services de veille traduit les inquiétudes des États, de la Commission européenne, de l'Alliance atlantique face au numérique. **La prise de conscience de la dangerosité des menaces sur l'Internet et *via* les modes d'échanges électroniques modernes constitue l'enjeu de la prochaine décennie.**

C. Le projet d'accord de libre-échange entre les États-Unis d'Amérique et l'Union européenne

Des garanties européennes et internationales devraient s'imposer pour la protection des données personnelles et la gouvernance de l'Internet avant que ne soient adoptées des clauses de l'accord de libre-échange relatives au numérique.
Bien plus, **le numérique ne devrait pas être inclus dans l'accord commercial car le numérique englobe le commercial et non le contraire**. L**e numérique pourrait justifier une exception numérique à l'instar de l'exception culturelle. En conséquence, ce secteur serait exclu des négociations commerciales**.

D. Vers une Europe du numérique cohérente ?

Lors du Conseil européen d'octobre **2013** sur l'économie numérique, **la France a défini trois priorités** : développer une stratégie industrielle européenne du numérique permettant l'**émergence d'acteurs européens innovants** ; garantir un **accès ouvert aux services et utilisateurs de l'Internet** ; **renforcer les règles de protection de la vie privée des citoyens européens** (encadrement des transferts de données en direction des États tiers, guichet unique de défense des droits des individus et des entreprises, coopération entre autorités de contrôle nationales sur les décisions de traitement des données personnelles).

E. Souveraineté et numérique

Devant l'ampleur possible des dégâts des attaques numériques, **les États se doivent de concevoir la protection des infrastructures critiques de la société, celle des opérateurs d'importance vitale (OIV) comme celle des citoyens reliés à eux de manière critique**.
Les notions de **détection des vulnérabilités** et de **résilience**, face et à la suite d'attaques numériques, sont essentielles.

II. LE CADRE NATIONAL DE LA MISE EN ŒUVRE DE LA SÉCURITÉ NUMÉRIQUE

A. Numérique et libertés

Le Conseil d'État préconise le développement d'un droit souple (**recommandations**, **guides de bonnes pratiques**, homologation des **codes de conduite professionnelle**, **certification** ou **médiation),** un droit ajustable et réversible en fonction de l'usage.
L'Union européenne entend affirmer ses valeurs sans imposer des règles désavantageant ses citoyens ou ses entreprises et donc en posant la territorialité de la norme.

B. La mise en œuvre opérationnelle de la sécurité numérique

Elle est assurée par la conjugaison des moyens de l'établissement **DGA Maîtrise de l'information** (Direction générale de l'armement, DGA), du **Centre d'analyse de lutte informatique défensive** (CALID), de la **brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI)** de la Gendarmerie nationale, de l'**Agence nationale de la sécurité des systèmes d'information (ANSSI) et par les industriels (*ICASI*, CIGREF, etc.).**

C. Organisation de la sécurité numérique

En matière de cybercriminalité, une difficulté majeure résulte de l'absence de lien entre le lieu de l'infraction et son auteur. En effet, le principe d'échange de Locard (l'utilisation de traces comme preuves) ne vaut pas pour la cybercriminalité : l'attaquant peut avoir agi aussi bien sur les lieux de l'infraction qu'avoir rebondi de site en site et de pays en pays. **La perte de ce lien géographique exige une coopération entre les polices internationales.**
De leur côté, **les assureurs et réassureurs répugnent à s'emparer du marché du risque numérique** (les risques antérieurs ne permettant pas de prévoir les risques futurs ; le calcul de la prime d'assurance étant quasi impossible : une entreprise a-t-elle mis en œuvre toutes les mesures de sécurité numérique possibles ?).

D. Les opérateurs d'importance vitale (OIV)

La sécurité numérique des plus de deux cents opérateurs d'importance vitale recensés en France, (la moitié appartenant au secteur privé) **nécessite une anticipation méthodique** (**cartographie des risques numériques, plan annuel de sécurité des systèmes d'information** incluant les systèmes d'information de gestion, industrielle – systèmes de commande ou *SCADA* –, les applications et les utilisateurs).
Le secteur des télécommunications comme celui de l'énergie privilégient la capacité de réaction (organisation agile aux cycles de décision courts, dirigeants et collaborateurs impliqués et pragmatiques), une **protection conçue dans la profondeur** et un **partage rapide de toute information en cas de crise**.
De fortes réticences existent face à l'informatique en nuage public (*cloud computing*) à laquelle seules des données secondaires peuvent être confiées.

III. La complexité du numérique rend sa sécurité pour les entreprises difficile à concevoir

A. Vers une représentation du numérique de nature à faciliter sa connaissance

Le numérique, réseau des réseaux – incluant tous les objets et outils qui y sont liés – **est immense, dynamique et omniprésent, impliqué dans tous les échanges**, humains ou technologiques. **Le numérique n'a pas de forme finie.** Néanmoins, **en matière de sécurité, la représentation du système est une condition essentielle à un usage responsable**, ce qui suppose de **s'interroger sur la manière dont les ordinateurs et les réseaux sont reliés entre eux**, d'un continent à l'autre, dont les informations sont acheminées, etc. **La sécurité du numérique est transversale et mêle militaire et civil, professionnel et personnel**.

B. Les infrastructures du numérique

Les infrastructures de noms de domaine, de routage, de messagerie, de navigation (moteurs de recherche), de nuage numérique – reposant sur le réseau Internet (non fiable) et impliquant des applications, parfois des applications métier, sont exposées à des **risques de cyberattaque.**

IV. Forces et faiblesses du système d'information de l'entreprise

A. Les trois niveaux de l'entreprise

L'entreprise fonctionne à partir des systèmes de décision, d'information et de communication, de production.

B. Analyse critique du système d'information de l'entreprise

Le numérique a profondément modifié et amélioré chacun de ces systèmes (réseau local de l'entreprise, avec ou sans fil) tout en y apportant des **fragilités pas toujours perçues et encore moins corrigées**. La multiplication des capteurs comme la confusion entre espaces de stockage personnels et espaces professionnels, le partage indifférencié des données introduisent de **nombreuses possibilités d'usages non souhaités**. De plus, **le monde de l'informatique industrielle et celui de l'informatique générale, de plus en plus interconnectés, accroissent ainsi le nombre d'entrées dans le système industriel**.

V. La sécurisation du système d'information d'une entreprise

A. Principes de sécurité d'un système d'information

Le déploiement pragmatique massif des équipements numériques dans les entreprises n'a pas été accompagné de la mise en place d'une surveillance par conception.

Or un système d'information doit assurer et maintenir les propriétés de **disponibilité, d'intégrité et de confidentialité (DIC)** à partir de la mise en œuvre des **fonctions de prévention, de surveillance, d'analyse, de réaction, d'investigation et de répression** dans le cadre d'un **processus d'amélioration continue de la sécurité en anticipation des attaques ou en réaction**.

Dans cet affrontement entre individus et cybernétiques, **l'inventivité caractérise l'humain**. **Faute de maîtriser l'introduction de machines dans cette spirale, le risque d'une perte totale du contrôle du système d'information existe**.

Les politiques de sécurité numérique des entreprises doivent s'inscrire dans le cadre de la Politique de Sécurité des Systèmes d'Information de l'État (PSSIE) – circulaire du Premier ministre du 17 juillet 2014 – fondée sur : des **opérateurs de confiance**, une **analyse de risque**, la **planification des ressources** pour la sécurisation, une **authentification forte**, la **labellisation par l'ANSSI** des produits informatiques, la **localisation sur le territoire national des données sensibles**.

B. Mise en œuvre de la prévention dans le système d'information d'une entreprise

À partir d'une ligne de **défense périmétrique** (pare-feu), des **zones d'accès** sont définies en fonction de la sensibilité des ressources à protéger, des **antivirus** installés, des **authentifications fortes** utilisées (internes et externes), les **identités gérées**, la **cryptographie** mise en œuvre, des **tunnels d'interconnexion sécurisés** (réseaux virtuels).

S'il n'existe pas de menace spécifique au nuage informatique – qui les comporte déjà toutes – généralement cet environnement amplifie les risques.

La difficile gestion des objets connectés, **conçus au mépris de mécanismes sérieux de sécurisation**, constitue une préoccupation majeure d'autant que **ces objets sont déjà présents sur des sites industriels de criticité élevée**.

VI. Les failles et les attaques numériques compromettant la sécurité des entreprises

A. Un milieu hostile

Les vulnérabilités (dont les portes dérobées) et les menaces doivent être divulguées et analysées pour que des parades soient conçues au plus tôt grâce à une **veille permanente** (tests d'intrusion). **Les *CERT/CC*** (*Computer Emergency Response Team Coordination Center*), dont l'ANSSI, organismes spécialisés et agréés, **interviennent en urgence sur les incidents de sécurité informatique**.

L'analyse de risques (évaluation des impacts et des probabilités d'occurrence d'un scénario), fondée sur une **cartographie du système,** tend à rendre les activités d'une entreprise les plus sûres possible, même si **la sécurité complète ne peut être garantie**.

Les entreprises n'ayant pas les moyens de mener ce type d'audit seraient intéressées par des chartes types peu coûteuses.

B. Les attaques contre le système d'information

Tout ne saurait être qualifié d'attaque numérique ; les chiffres cités à cet égard sont souvent très exagérés.
Anecdotiques il y a quelques années, **certaines attaques deviennent extrêmement professionnelles et se généralisent**. **Les attaques complexes comprennent une phase préalable d'ingénierie sociale.**
Elles ne sont pas toutes l'œuvre d'informaticiens extrêmement compétents, d'autant que des logiciels de piratage grand public commencent à apparaître.
La spécificité du risque numérique fait qu'une entreprise peut ignorer, parfois durant des années, une attaque informatique en cours ou ne pas percevoir les conséquences à long terme d'une agression.

C. La fonction de surveillance de la sécurité

La supervision de la sécurité repose sur **l'analyse des traces** provenant des systèmes de détection d'intrusion placés à divers endroits du système d'information pour en assurer la surveillance.
Le système de gestion des informations et événements de sécurité (*SIEM*) gère ces traces et les interprète.

La création d'un centre de sécurité opérationnelle (*Security Operations Center* ou *SOC*) n'est accessible qu'à de grandes entreprises tandis que les autres recourent à des experts extérieurs comme l'ANSSI, la DGA, etc.

VII. La culture du numérique et l'éducation à sa sécurité

A. Temps et contretemps de la sécurité numérique

Le décalage entre le recours permanent à l'outil numérique en devenir et le manque de maîtrise de cet outil laissent les entreprises désemparées, alors que les évolutions de cette situation s'inscrivent dans des calendriers multiples et parfois contradictoires.
Le temps a manqué pour une observation, voire une réflexion, *a fortiori* pour une éducation et la construction d'une culture du numérique.
Or, **toutes les entreprises ont besoin d'un numérique sûr** – c'est leur système nerveux qui ne peut être affecté sans compromettre leur existence.
L'ANSSI et des groupements d'entreprises ont élaboré des méthodes et des guides pour aider les entreprises à bâtir leur sécurité numérique de manière rapide, cohérente et efficace dans le **respect de règles d'hygiène informatique.**
Un autre contretemps résulte de la **coexistence, pour l'heure non convergente, de priorités mondiales** (gouvernance mondiale de l'Internet), **internationales** (projet de Traité économique de partenariat transatlantique dit *TAFTA*), **européennes** (projet de règlement et projet de directive européens en gestation) et **nationales** (projet de loi sur le numérique). Compte tenu du caractère vital du numérique, **la question de l'exigence de l'affirmation d'une exception numérique dans les négociations internationales est posée**.

B. Les acteurs de la sécurité numérique

En complément du plan national de cyberdéfense et ses Pacte Défense cyber 2016 et Pacte défense PME (portant sur la formation, la recherche ou les entreprises), et du plan cybersécurité parmi les plans de la Nouvelle France industrielle, le **Gouvernement** a incité à la création du **club des industriels de la cyberdéfense** et à l'émergence d'une **communauté nationale de cyberdéfense**. Cela complète l'action de la **CNIL** et de l'**ANSSI** comme celles des **entreprises** (dont le **CoFIS**, le **CIGREF, le CLUSIF,** etc.**)** concourant à **instaurer une hygiène informatique en conjuguant cybersécurité et cyberdéfense.**

C. Faire de l'économie avec du droit ?

Une fois analysé, le risque numérique peut constituer une opportunité aux retombées non négligeables grâce au développement d'atouts français (en matière de formation, d'audits de sécurité numérique, de cartographie des risques, de cryptographie, de sondes souveraines, de détecteurs d'intrusion, etc.) pour construire « *la France de la sécurité et de la confiance numérique* » au moyen d'une industrie performante en matière de cybersécurité.
Au-delà d'une science ou d'une technologie numérique imposant leur logique binaire, **la réduction du risque numérique passe aussi par la sensibilisation, l'éducation, l'acquisition de réflexes, d'un savoir se comporter face au numérique. Le tout sans perdre de vue l'évolution rapide du contexte international dans lequel ces avancées doivent s'inscrire.**

Pour consulter le rapport :
www.assemblee-nationale.fr/commissions/opecst-index.asp
www.senat.fr/opecst

Avril 2015

Sénat - 15 rue de Vaugirard 75291 Paris Cedex 06 - Tel: 01 42 34 25 58 - Fax : 01 42 34 46 04
Assemblée nationale - 101, rue de l'Université - Bât F. - 75355 Paris 07 SP - Tel: 01 40 63 70 65 - Fax: 01 40 63 70 95
www.assemblee-nationale.fr - www.senat.fr