Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Centre d'analyse stratégique

Mars 2013
n° 324
LA NOTE D'ANALYSE
Développement durable

Cybersécurité*, l'urgence d'agir

Les attaques informatiques se multiplient et se complexifient sous l'effet du développement du cyberespionnage, de la cybercriminalité et d'États qui utilisent ces attaques à des fins stratégiques. Parallèlement, des usages nouveaux (*cloud computing*, mobilité) accroissent les vulnérabilités des systèmes d'information.

Confrontés à cette menace, les entreprises, les administrations et *a fortiori* les particuliers sont soit désarmés, soit peu conscients des risques encourus et de leurs conséquences économiques et financières. Des attaques informatiques peuvent piller le patrimoine informationnel des entreprises et toucher des infrastructures stratégiques. Le Livre blanc sur la défense et la sécurité nationale paru en 2008 avait ainsi consacré la sécurité des systèmes d'information comme l'une des quatre priorités stratégiques pour la France : c'est un enjeu de compétitivité et de souveraineté nationale.

Pour élever le niveau de sécurité, tout en tirant profit des avantages d'un Internet ouvert et décentralisé, les organisations doivent adopter une démarche rationnelle d'analyse de risques afin de mettre en œuvre une réponse adaptée sur le plan technique et organisationnel. L'offre nationale de solutions de sécurité doit également se structurer pour permettre une meilleure valorisation des compétences technologiques françaises et garantir un plus haut degré de souveraineté. ■

PROPOSITIONS

1. **Renforcer les exigences de sécurité imposées aux opérateurs d'importance vitale (OIV), sous le contrôle de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).**
2. **Développer et mettre à la disposition des petites et moyennes entreprises des outils simples pour gérer les risques.**
3. **Élargir les missions de l'ANSSI pour accompagner le développement de l'offre française de solutions de cybersécurité.**
4. **Revoir le cadre juridique afin de conduire, sous le contrôle de l'ANSSI et d'un comité d'éthique *ad hoc*, des expérimentations sur la sécurité des logiciels et les moyens de traiter les attaques.**

* Le préfixe "cyber" se réfère, dans son acception actuelle, aux systèmes d'information. Ainsi, le terme "cybersécurité" doit-il être compris comme la sécurité des systèmes d'information.

LES ENJEUX

L'essor des technologies de l'information a entraîné une dépendance croissante à l'égard des outils numériques. En raison des enjeux économiques et politiques sous-jacents, les attaques informatiques se sont considérablement développées et sophistiquées au cours des dernières années. Leurs auteurs sont techniquement difficiles à identifier, et l'investissement et le risque pénal encouru sont relativement faibles au regard des gains potentiels.

La découverte en 2010 du ver informatique Stuxnet, conçu pour saboter le processus d'enrichissement d'uranium iranien, a fait prendre conscience de la possibilité de "cyberattaques" contre des infrastructures physiques. Les organisations sont aussi confrontées à un "cyberespionnage" généralisé, qui vise leur patrimoine informationnel stratégique (activités de R & D, informations financières et commerciales, etc.). Ainsi, assurer un certain niveau de sécurité des systèmes d'information est-il devenu un enjeu de première importance.

En France, la création en 2009 de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) témoigne d'une prise de conscience de ces questions. Cependant, comme le souligne le rapport sénatorial de juillet 2012 sur la cyberdéfense[1], le niveau de sécurité des systèmes d'information des organisations reste globalement insuffisant malgré les efforts fournis.

La présente *Note d'analyse* fait le point sur l'état des menaces informatiques et sur les réponses apportées en France et à l'étranger. Elle formule ensuite des recommandations destinées à élever le niveau de cybersécurité.

UN "CYBERESPACE" VULNÉRABLE, EN PROIE À DES ACTES DÉLICTUEUX CROISSANTS

Les attaques informatiques se complexifient et se professionnalisent

Des attaques à visées stratégiques

La découverte du programme malveillant Stuxnet en 2010 a révélé l'existence d'attaques informatiques d'une ampleur jamais atteinte jusqu'alors. Grâce à de nombreuses failles de sécurité, Stuxnet s'est attaqué au programme d'armement nucléaire iranien, en sabotant le processus d'enrichissement de l'uranium. Son avancée technologique est telle qu'elle équivaudrait, selon un chercheur ayant étudié l'attaque, à *"l'arrivée d'un avion de chasse de dernière génération sur un champ de bataille de la Première Guerre mondiale"*[2].

Le ver Flame, découvert en 2012, constitue quant à lui le système d'espionnage informatique le plus sophistiqué jamais découvert à ce jour. Contrôlé à distance, il est, entre autres, capable de copier tous types de fichier, de mémoriser les frappes sur le clavier, de déclencher le micro et l'émetteur Bluetooth, et peut s'autodétruire à tout moment.

Ces exemples témoignent d'un affrontement d'un type nouveau : des cyberattaques peuvent être dirigées contre des infrastructures physiques[3] (réseaux de distribution d'énergie, infrastructures de transport, chaînes de production, etc.) ou participer à des opérations de renseignement. Dans certains cas, leur niveau de sophistication est tel que seules des puissances étatiques seraient en mesure de les produire. **L'appropriation par les États des attaques informatiques à des fins stratégiques conduit à une "course à l'armement" susceptible d'augmenter le niveau général de la menace.**

Un développement préoccupant du cyberespionnage

Les attaques informatiques destinées à s'approprier des informations sensibles (parfois appelées APT : *Advanced Persistent Threats*) connaissent un développement important et constituent une menace pour les entreprises et les administrations[4]. Les attaquants sont à la recherche de données stratégiques :

– informations liées à la recherche et au développement ;

– informations échangées par les dirigeants ;

– données financières et commerciales : contrats, négociations en cours, etc.

(1) Bockel J.-M. (2012), *Rapport d'information sur la cyberdéfense*, commission des Affaires étrangères, de la Défense et des Forces armées, Sénat.
(2) Langner R. (2010), *The big picture*.
(3) ANSSI (2012), *La cybersécurité des systèmes industriels*.
(4) Duluc P. (2012), "Les menaces sur le cyberespace : une réalité", *Revue de l'électricité et de l'électronique*, n° 2, p. 16-20.

Noyées dans le flot des données échangées, ces attaques peuvent rester invisibles pendant plusieurs années et entraîner un espionnage économique massif. Ainsi l'entreprise d'équipements de télécommunications Nortel a été victime d'un espionnage généralisé à partir du début des années 2000, les pirates ayant eu accès à la totalité des documents techniques, financiers et de R & D pendant près de dix ans[5]. Il s'agit très probablement de l'une des principales causes de la faillite de l'entreprise en 2009.

En 2010, le ministère français de l'Économie et des Finances a subi une campagne d'attaque de ce type. Environ 150 ordinateurs, principalement au sein de la direction générale du Trésor, ont été infectés, sur les quelque 170 000 ordinateurs du ministère, ce qui illustre le degré de précision du cyberespionnage. L'attaque avait notamment pour but de recueillir des informations relatives à la présidence française du G8 et du G20[6].

Des quotidiens américains, parmi lesquels le *New York Times* et le *Wall Street Journal*, ont annoncé en janvier 2013 avoir été victimes d'espionnage de grande ampleur (vol de mots de passe, d'emails et de données de journalistes), accusant des pirates basés en Chine.

La plupart des grandes entreprises et des administrations ont très probablement été victimes d'intrusions à des fins d'espionnage. Cependant, hormis ces quelques exemples, il n'est pas facile de recenser ces attaques en raison de la réticence des organisations à les révéler.

La professionnalisation de la cybercriminalité

La cybercriminalité désigne l'ensemble des infractions pénales commises *via* les réseaux informatiques (vols de données à caractère personnel ou industriel, fraude ou vol d'identifiants bancaires, diffusion d'images pédophiles, atteinte à la vie privée, etc.). **Encouragé par l'importance des sommes en jeu pour un risque relativement faible, le crime organisé s'est emparé de la cybercriminalité.** Selon les estimations de Norton[7], le coût financier de la cybercriminalité atteindrait en 2012 110 milliards de dollars, dont 42 % liés à des fraudes, 17 % à des vols ou pertes de données et 26 % aux frais de réparation. Le trafic de drogue (cannabis, cocaïne et héroïne) représenterait 288 milliards de dollars, selon la même étude.

Un nombre d'attaques amené à croître

Le nombre d'attaques et leur intensité devraient augmenter. La dissémination de codes malveillants entraîne des effets collatéraux, voire "boomerang". À titre d'exemple, des fonctions élémentaires du ver Stuxnet sont disponibles à la vente sur Internet et peuvent être utilisées à des fins malveillantes. Si les techniques d'attaque classiques sont toujours très utilisées et peuvent se combiner de manière complexe, des menaces nouvelles devraient se développer (cf. encadré 1).

Encadré 1

Techniques d'attaques les plus fréquentes[8]

– Le déni de service : saturation d'un réseau ou d'un service par un envoi de requêtes en très grand nombre afin d'empêcher ou de limiter fortement sa capacité à fournir le service attendu[9]. De telles attaques ont par exemple paralysé les sites institutionnels d'Estonie en 2007 ;
– Le piégeage de logiciels : utilisation de programmes malveillants (virus, ver, cheval de Troie, etc.) pour perturber le fonctionnement d'un logiciel et infecter un système d'information ;
– Les techniques d'ingénierie sociale : acquisition déloyale d'information afin d'usurper l'identité d'un utilisateur. Parmi ces techniques, l'hameçonnage (phishing) consiste par exemple à faire croire à la victime qu'elle s'adresse à un tiers de confiance (banque, administration, etc.) afin de lui soutirer des renseignements personnels[10].

Exemples de nouveaux types d'attaques[11] :

– Attaques des couches basses des réseaux ;
– Rançongiciels : logiciels malveillants qui "prennent en otage" des données personnelles et exigent une rançon pour leur restitution.

Des vulnérabilités nouvelles à prendre en considération

La sécurité, frein à l'adoption du *cloud computing*

Le *cloud computing* [12] consiste à utiliser des serveurs à distance, accessibles par Internet, pour traiter ou stocker de l'information. Il **connaît un développement massif**[13] en raison de ses nombreux avantages : baisse des coûts

(5) Gorman S. (2012), "Chinese hackers suspected in long-term Nortel breach", *The Wall Street Journal*, 14 février.
(6) Cf. le rapport Bockel *(op. cit.)* pour une description plus détaillée de l'attaque.
(7) Norton (2012), *2012 Norton cybercrime report*, juillet.
(8) Pour une présentation exhaustive des menaces, consulter le guide de l'ANSSI : "Menaces sur les systèmes informatiques".
(9) http://www.securite-informatique.gouv.fr/gp_rubrique33.html
(10) http://fr.wikipedia.org/wiki/Hame%C3%A7onnage
(11) ANSSI (2011), Cyberconflits, quelques clés de compréhension.
(12) Ou "informatique en nuage", en français.
(13) Selon Gartner, le marché du *cloud computing* devrait représenter 150 milliards de dollars en 2014.

liée à la mutualisation des ressources, facturation à l'usage, puissance de calcul quasi-illimitée, travail collaboratif facilité, mobilité, évolutivité. **Cependant, il n'offre pas encore toutes les garanties de sécurité pour sa pleine appropriation.** En effet, le *cloud computing* comporte des risques organisationnels, techniques et juridiques, susceptibles de compromettre la confidentialité, l'intégrité et la disponibilité des données déportées.

Le déplacement de tout ou partie du système d'information hors du champ de contrôle de l'organisation crée un risque de perte de gouvernance. Sur le plan technique, les processus d'authentification des utilisateurs et de gestion des droits d'accès posent également des problèmes de sécurité. En juillet 2012, l'entreprise Dropbox a ainsi reconnu que des mots de passe volés sur d'autres sites Internet avaient permis à des pirates d'accéder à des documents stockés sur les serveurs de l'entreprise[14]. Enfin, l'incertitude sur la localisation des données hébergées sur le *cloud* est un facteur d'insécurité juridique : il est difficile de déterminer quel régime juridique sera applicable en cas de litige.

La mobilité et les nouveaux usages génèrent des vulnérabilités dans les systèmes d'information

Le développement des terminaux (ordinateurs portables, smartphones, tablettes) et des réseaux mobiles (3G, 4G, Wifi) offre aux membres d'une organisation un accès étendu à ses systèmes d'information. Les directeurs des systèmes d'information (DSI) constatent une forte demande des employés pour ces outils de mobilité[15]. Cependant, **en bouleversant les systèmes d'information de l'entreprise, la mobilité génère des risques pour la sécurité** :

– moins matures en matière de sécurité, les smartphones et les tablettes sont aussi moins bien intégrés au système d'information de l'entreprise[16] ;

– le rythme d'innovation très élevé des applications mobiles, et les nouveaux usages qui y sont associés, entraînent de nombreuses failles et vulnérabilités potentiellement exploitables[17] ;

– la prédominance de l'offre américaine et asiatique de terminaux mobiles (Samsung, Apple, Sony, HTC, RIM, Huawei, ZTE, etc.) constitue un risque pour la France et les pays européens qui ne peuvent garantir leur intégrité technique.

Encadré 2

Le "BYOD", une pratique antinomique à la maîtrise de la sécurité

Le BYOD, sigle provenant de l'expression anglaise *"Bring your own device"* (" apportez votre propre appareil"), consiste à utiliser un terminal mobile personnel à des fins professionnelles[18].

En fort développement ces dernières années, le BYOD est extrêmement complexe à gérer pour les responsables de la sécurité :

– la sécurité des terminaux est difficile à garantir, en raison de la diversité des appareils et des systèmes d'exploitation, des vulnérabilités causées par les usages privés (débridage d'OS, installation d'applications, etc.) et de l'enchevêtrement entre données privées et professionnelles ;

– la connexion des terminaux privés aux systèmes d'information de l'entreprise pose la question de l'authentification et de la protection des données sensibles de l'entreprise ;

– l'absence de cadre juridique définissant les obligations et prérogatives des employés et des entreprises expose les différentes parties prenantes au risque juridique.

Beaucoup considèrent néanmoins que le BYOD ne représente qu'une diversification inévitable des terminaux, qui se gère très bien en sécurisant les accès distants. Il suffit de changer de postulat : désormais, les terminaux ne sont pas forcément de confiance.

Procédés industriels, Internet des objets : les vulnérabilités informatiques s'étendent au monde réel

L'utilisation massive des technologies de l'information dans tous les secteurs de l'économie a généré des interactions croissantes entre les mondes virtuel et réel. Les infrastructures physiques sont désormais très souvent contrôlées à distance par **des logiciels de supervision et de contrôle** (SCADA, *Supervisory control and data acquisition*), **qui peuvent être vulnérables aux attaques informatiques** pour plusieurs raisons :

– les besoins de consolidation des données et la pression à la baisse des coûts ont poussé à la convergence des technologies et "ont apporté aux systèmes industriels les vulnérabilités du monde de l'informatique de gestion"[19] ;

– les mises à jour et les correctifs destinés à améliorer la sécurité des logiciels sont difficilement applicables en raison de contraintes de fiabilité et de disponibilité des systèmes industriels.

(14) https://blog.dropbox.com/2012/07/security-update-new-features/

(15) Akella J. et *al.* (2012), "Mobility disruption: a CIO perspective", *McKinsey Quarterly* (Traduction française dans la ParisTech Review).

(16) CIGREF (2010), Sécurisation de la mobilité, octobre.

(17) Akella et *al.* (2012), *op.cit.*

(18) On parle de manière plus générale de "consumérisation de l'informatique" lorsque des technologies adoptées par le grand public sont ensuite utilisées dans le cadre de l'entreprise.

(19) ANSSI (2012) *op. cit.*

Le développement de l'Internet des objets devrait multiplier les interactions entre mondes virtuel et réel et étendre le risque d'attaque. Selon Cisco, environ 50 milliards d'objets devraient être connectés à Internet en 2020[20]. Dans le secteur de la santé par exemple, les stimulateurs cardiaques *(pacemaker)* connectés permettent de transmettre des données relatives à l'activité cardiaque pour une surveillance à distance en temps réel. Un chercheur[21] a démontré pouvoir prendre le contrôle d'un *pacemaker* à distance (à une dizaine de mètres) et déclencher des chocs électriques mortels (830 volts).

Un niveau de sécurité très variable selon les entreprises et les administrations

Les organisations appréhendent difficilement le risque informatique et y sont peu sensibilisées

Avec la numérisation croissante des activités, **les systèmes d'information des organisations se complexifient et doivent répondre à des usages et des besoins de plus en plus variés**. Les évolutions que subissent les organisations (fusions-acquisitions d'entreprises, restructurations de départements ministériels…) ajoutent un degré supplémentaire de complexité.

Les dépenses de sécurité informatique sont trop souvent considérées comme une variable d'ajustement et fortement contraintes dans le contexte de maîtrise des coûts. Le montant des investissements nécessaires pour assurer la sécurité des systèmes d'information[22] est connu et immédiat : selon les chiffres communément admis, il représenterait en moyenne entre 0,5 % et 2 % du chiffre d'affaires des entreprises[23]. En revanche, le coût économique de l'insécurité numérique est incertain, lointain, et souvent sous-estimé. Pourtant, des attaques informatiques peuvent entraîner des pertes financières, nuire à l'image de l'organisation et potentiellement mettre en péril son activité.

Les administrations sont très exposées même si leur niveau de sécurité s'améliore

Le niveau de maturité des réflexions par rapport au risque et les niveaux de sécurité restent très hétérogènes selon les ministères[24]. La campagne d'attaque qu'a subie le ministère de l'Économie et des Finances en 2010 (cf. ci-dessus) est symptomatique de la complexité et de la non-maîtrise des systèmes d'information publics.

Les équipes d'intervention de l'ANSSI ont d'abord dû reconstituer la cartographie du réseau du ministère qui n'en disposait pas afin notamment de recenser ses portes d'entrée et de sortie vers Internet. D'autres ministères ou institutions de la République sont, ou ont été, victimes d'attaques informatiques d'importance.

Alertés par le niveau de la menace et conscients de la nécessité de sécuriser les informations sensibles, les pouvoirs publics ont entrepris de réformer en profondeur les systèmes d'information ministériels. Le Conseil des ministres du 25 mai 2011 a décidé de la création d'un Réseau Interministériel de l'État (RIE), réseau sécurisé regroupant l'ensemble des réseaux des ministères et permettant la continuité de l'action gouvernementale en cas de dysfonctionnement grave d'Internet. Conduit par la DISIC[25] et devenu Service à compétence nationale, ce projet a intégré la sécurité dès l'origine, sur le principe d'une "défense en profondeur des couches basses des réseaux". La migration progressive des différents réseaux ministériels vers le RIE va permettre une meilleure maîtrise de l'architecture et une homogénéisation de la sécurité des administrations.

Les opérateurs d'importance vitale (OIV), livrés à eux-mêmes, présentent une grande disparité face aux risques

Le développement récent d'attaques informatiques contre des infrastructures physiques souligne l'importance et l'urgence d'améliorer leur protection. La législation a identifié des opérateurs dits d'importance vitale (OIV) auxquels elle impose des dispositifs de sécurité spécifiques (cf. encadré 3).

Encadré 3

Les opérateurs d'importance vitale

Selon le Code de la défense, les opérateurs d'importance vitale sont ceux qui exploitent "des établissements dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation".
Douze secteurs d'activité ont été identifiés comme étant d'importance vitale :

Secteurs étatiques :
– activités civiles de l'État ;
– activités militaires de l'État ;
– activités judiciaires ;
– espace et recherche.

(20) Cisco (2011), *The Internet of Things*, White Paper.
(21) Barnaby Jack a présenté ce travail lors de la conférence "Breakpoint Ruxcon" à Melbourne en 2012.
(22) Moyens humains, achat de produits et de services de sécurité, mise en place d'une démarche d'analyse de risque, etc.
(23) Le budget TIC représente en moyenne 5 % à 10 % du chiffre d'affaires, et les dépenses consacrées à la sécurité sont d'environ 15 % à 20 % de ce budget. Cependant, il n'y a pas forcément de corrélation entre les montants dépensés et la qualité de la protection des systèmes d'information.
(24) Pour une explication de l'organisation de la politique de sécurité des systèmes d'information ministérielle, voir http://www.ssi.gouv.fr/fr/ssi/la-ssi-en-france/.
(25) La Direction interministérielle des systèmes d'information et de communication (DISIC) est rattachée au Secrétariat général pour la modernisation de l'action publique (SGMAP) créé par décret le 30 octobre 2012.

Secteurs de la protection des citoyens :
– santé ;
– gestion de l'eau ;
– alimentation.

Secteurs de la vie économique et sociale de la nation :
– énergie ;
– communication, électronique, audiovisuel et information ;
– transports ;
– finances ;
– industrie.

Pour chaque secteur d'activité, les opérateurs d'importance vitale (OIV) sont désignés par arrêté ministériel. En 2010, environ 250 OIV étaient répertoriés sur le territoire national[26]. Ils sont soumis à des obligations particulières : formation des responsables, analyse de risque, identification de points d'importance vitale qui feront l'objet d'un plan particulier de protection (PPP) et d'un plan de protection externe (PPE), etc.

Cependant, les risques relatifs aux systèmes d'information restent un objectif secondaire et ne font pas l'objet d'une législation contraignante en matière de sécurisation. L'ANSSI ne dispose, vis-à-vis des OIV, que d'un rôle de conseil et la sécurité de ces infrastructures vitales est très variable.

La sensibilisation à la sécurité informatique est très variable selon les entreprises

La prise de conscience du niveau de la menace par les grandes entreprises est également très variable. Selon une enquête réalisée par le Club de la sécurité de l'information français (CLUSIF), 63 % des entreprises de plus de 200 salariés[27] ont formalisé une politique de sécurité de l'information, mais seulement 14 % d'entre elles évaluent systématiquement les impacts financiers des incidents de sécurité (25 % le font parfois). Selon les responsables de la sécurité des systèmes d'information (RSSI), les principaux freins à la conduite de leurs missions sont le manque de budget et les contraintes organisationnelles.

Il est beaucoup plus difficile de dresser un bilan du niveau de cybersécurité des très petites, petites et moyennes entreprises (TPE/PME) et des entreprises de taille intermédiaire (ETI). L'approche de la sécurité dépend en grande partie de la sensibilité des dirigeants pour ces questions. La démarche de l'ANSSI, qui vient de publier un guide[28], est très certainement utile pour les sensibiliser et assurer un niveau de sécurité minimal. Cependant, ces dispositions ne sont pas suffisantes pour mettre en œuvre une véritable politique de sécurité adaptée au niveau de risque auquel les TPE/PME/ETI peuvent parfois être confrontées, en particulier si leur activité appartient à des secteurs critiques.

La sécurisation des terminaux individuels est un enjeu majeur pour réduire le niveau général de la menace

Les particuliers possèdent de plus en plus de terminaux connectés à Internet, que des attaques informatiques (ver, cheval de Troie) peuvent infecter. Les pirates informatiques prennent le contrôle de ces machines et peuvent alors former des réseaux d'ordinateurs *(botnets)* destinés à mener des actions malveillantes de grande ampleur (*spam*, *phishing*, déni de service, fraude au clic, etc.). Des ordinateurs mal protégés permettent donc aux pirates d'étendre leurs capacités d'action.

Le risque lié aux terminaux mobiles est toujours mal apprécié : seulement 38 % des personnes interrogées par le CLUSIF (et 24 % des 15-24 ans) sont conscientes que le téléchargement d'applications et d'utilitaires sur smartphones et tablettes est un facteur de risque supplémentaire.

LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, UNE PRIORITÉ STRATÉGIQUE MONDIALE

Depuis 2008, la France a assigné à la sécurité des systèmes d'information une priorité stratégique

Les pouvoirs publics ont progressivement pris conscience de l'importance de garantir la sécurité des systèmes d'information. En 2006, un rapport parlementaire[29] constatait à cet égard le retard préoccupant pris par la France. À partir de 2008, une démarche politique est véritablement lancée, **avec la publication du Livre blanc sur la défense et la sécurité nationale**[30], qui consacre la sécurité des systèmes d'information "enjeu de souveraineté nationale". En 2009, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est créée en remplacement de la DCSSI. "Autorité nationale en matière de sécurité des systèmes d'information" et rattachée au Secrétaire général de la défense et de la sécurité nationale (SGSDN), ses principales missions[31] sont :

(26) Boutant M. et Garriaud-Maylam J. (2010), *Rapport d'information sur l'utilisation des réserves militaires et civiles en cas de crise majeure*, commission des Affaires étrangères, de la Défense et des Forces armées, Sénat.
(27) CLUSIF (2012), *Menaces informatiques et pratiques de sécurité en France*.
(28) ANSSI (2013), *Guide d'hygiène informatique*.
(29) Lasbordes P. (2006), *La sécurité des systèmes d'information : un enjeu majeur pour la France*, La Documentation française.
(30) *Défense et Sécurité nationale : le Livre blanc* (2008), La Documentation française.
(31) L'ANSSI délivre aussi des labels de sécurité à des produits et à des prestataires de services de confiance, participe au travail réglementaire et produit des guides de recommandations et de bonnes pratiques en matière de SSI.

– d'assurer la sécurité des systèmes d'information de l'État ;
– de veiller à celle des OIV ;
– de coordonner les actions de défense des systèmes d'information ;
– de concevoir et déployer les réseaux sécurisés des hautes autorités de l'État.

Depuis sa création, les ressources de l'ANSSI ont régulièrement augmenté pour accompagner l'élargissement de son champ de compétences[32]. Entre 2009 et 2012, le budget est passé de 45 à 75 millions d'euros, les effectifs ont plus que doublé (300 agents fin 2012) et cette croissance devrait se poursuivre en 2013.

En parallèle à cette mission interministérielle menée par l'ANSSI, **plusieurs ministères conduisent des actions spécifiques dans le domaine de la cybersécurité** :

– le **ministère de la Défense** : les volets technique et opérationnel sont respectivement conduits par la Direction générale de l'armement (DGA) et l'État-major des armées (EMA). Ce dernier s'est doté en juillet 2011 d'un Officier général chargé de la cyberdéfense et d'une structure opérationnelle d'expertise technique et de traitement des attaques, le Centre d'analyse de lutte informatique défensive (CALID) ;
– le **ministère de l'Intérieur** : la Direction centrale du renseignement intérieur (DCRI) et l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) sont actifs dans la lutte contre l'espionnage et la cybercriminalité.

Malgré cette prise de conscience, le rapport parlementaire de juillet 2012[33] **souligne les lacunes du système français : la sécurité des administrations et des OIV est insuffisante et les effectifs et moyens consacrés à la sécurité sont nettement inférieurs à ceux déployés par nos principaux partenaires.**

Le caractère stratégique de la sécurité, un constat partagé par les pays développés

La sécurité des systèmes d'information est un enjeu reconnu à travers le monde, pour lequel les pays développés ont beaucoup investi ces dernières années.

Les États-Unis ont été l'un des premiers pays à se préoccuper de la protection de leurs systèmes d'information. Le gouvernement américain devrait consacrer 50 milliards de dollars à la cyberdéfense sur la période 2010-2015[34]. **Le développement de capacités d'attaque est l'une des principales caractéristiques de la doctrine américaine en matière de cybersécurité**[35]**.** Affirmant leur souveraineté, les États-Unis s'octroient aussi le droit de riposter à une cyberattaque par des armes conventionnelles[36].

Le Royaume-Uni fournit également un effort majeur : en novembre 2011, le gouvernement a publié une nouvelle stratégie de cybersécurité[37], soutenue par un **programme de financement d'environ 800 millions d'euros sur quatre ans, qui a pour objectifs d'améliorer la résilience aux cyberattaques et de créer un environnement sécurisé**.

De même, l'Allemagne renforce la résilience de ses infrastructures critiques et augmente les moyens mis à la disposition du BSI[38], équivalent de l'ANSSI (budget de 80 millions d'euros et effectifs de 560 agents en 2012, pour un éventail de missions plus réduit que celui de l'ANSSI).

Au niveau européen, l'ENISA *(European Network and Information Security Agency)*, créée en 2004, joue un rôle d'expertise et de soutien aux États membres en retard dans le domaine de la cybersécurité. La qualité des guides de procédure qu'elle produit est unanimement soulignée. L'agence n'a cependant pas de responsabilité opérationnelle en raison de la volonté des États membres de conserver leur souveraineté[39]. L'inauguration en janvier 2013 d'un Centre européen de lutte contre la cybercriminalité marque la **volonté de l'UE d'agir dans le domaine**. Identifiée comme une priorité, la cybersécurité fait l'objet d'un plan stratégique[40], présenté en février 2013, qui vise à maintenir un "cyberespace ouvert, sûr et sécurisé".

Au niveau international, les initiatives sont disparates et l'absence d'accord multilatéral témoigne des désaccords de fond entre les États sur la régulation des réseaux et la gouvernance d'Internet. L'Organisation des Nations unies (ONU) et l'Union internationale des télécommunications (UIT) font face à des blocages politiques. Le sommet de l'UIT en décembre 2012, à Dubaï, destiné à réviser le règlement des télécommunications interna-

(32) L'agence est devenue "Autorité nationale de défense des systèmes d'information" en 2011 et a vu ses pouvoirs renforcés vis-à-vis des opérateurs de communication électronique (OCE) en 2012 sous l'influence du droit européen (transposition du "Paquet Telecom").
(33) Voir Bockel (2012), *op. cit.*
(34) Voir Bockel (2012), *op. cit.*
(35) Le lieutenant-général des *Marines* a reconnu au cours d'une conférence avoir mené des cyberattaques en 2010 lors de la guerre en Afghanistan, *Huffington Post*, 24 août 2012.
(36) Discours de Leon Panetta, Secrétaire à la Défense, prononcé le 11 octobre 2012.
(37) *The UK cyber security strategy, Protecting and promoting the UK in a digital world*, novembre 2011.
(38) *Bundesamt für Sicherheit in der Informationstechnik*.
(39) La Commission européenne souhaite tout de même s'emparer de ce sujet de manière plus active et a lancé en 2012 une consultation publique ("Improving net-work and information security in Europe") pour réformer l'agence.
(40) Ce plan stratégique s'intitule : *"Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"*.

tionales (RTI), a été un échec, 55 pays (dont la France) n'ayant pas signé le projet de texte final. La Convention de Budapest sur la cybercriminalité (2001), premier traité international conclu dans le cadre du Conseil de l'Europe et qui tente de lutter contre la cybercriminalité, a perdu sa vocation universelle en raison du faible nombre de pays signataires (une cinquantaine d'États dont les États-Unis et les pays membres de l'Union européenne).

LA GESTION DES RISQUES : CONCILIER SÉCURITÉ, OUVERTURE DES SYSTÈMES D'INFORMATION ET PROTECTION DES LIBERTÉS INDIVIDUELLES

Élever le niveau de sécurité des systèmes d'information, un enjeu économique et de souveraineté majeur

Sur le plan économique, **l'amélioration du niveau de sécurité des systèmes d'information est un facteur de compétitivité et d'attractivité** qui permet :

– de mieux protéger le patrimoine informationnel des entreprises et des administrations ;

– d'apporter un supplément de confiance dans les technologies numériques susceptible de faciliter leur appropriation par les entreprises et les citoyens ;

– d'attirer des entreprises en procurant un avantage comparatif par rapport à des pays moins sécurisés.

Il s'agit aussi d'un enjeu de souveraineté nationale puisque la continuité de l'activité économique et des services publics dépend en partie du niveau de protection et de résilience des administrations et des OIV face aux attaques informatiques.

La recherche de la sécurité doit cependant être considérée parallèlement à d'autres objectifs : l'ouverture des systèmes d'information et la protection des libertés individuelles.

Isoler des systèmes d'information d'internet réduit de fait leur exposition aux attaques, même si le "risque zéro" n'existe pas[41]. De tels systèmes sécurisés sont nécessaires pour les installations devant être protégées, quelles que soient l'ampleur et l'intelligence de l'attaque. Eugène Kaspersky souligne ainsi qu'une solution consisterait à créer deux réseaux parallèles : l'un libre et ouvert, et un autre complètement sécurisé[42].

Ces dispositions ne doivent toutefois pas être généralisées, au risque de se priver des avantages économiques d'un Internet ouvert et décentralisé : diffusion de l'innovation, démocratisation des savoirs, libéralisation des échanges, amélioration de la productivité, etc.

De même, la sécurité des systèmes d'information instrumentalisée peut se transformer en "sécurité de l'information" et mettre en péril les droits et les libertés individuels. Détournés, les outils de sécurité utilisés pour la surveillance des réseaux et l'interception des communications peuvent comporter des risques pour la vie privée des citoyens. En France, la Commission nationale de l'informatique et des libertés (CNIL) évalue les mesures de sécurité à l'aune de leurs conséquences sur la protection de la vie privée et des libertés individuelles.

La gestion des risques : une approche rationnelle de la sécurité pour concilier ces différents objectifs

Les RSSI cherchent donc à concilier un haut niveau de sécurité, l'accès à Internet et la protection des libertés individuelles. Pour cela, les organisations doivent **adopter une démarche rationnelle et objective de gestion des risques**. Celle-ci a pour objectif d'identifier, d'analyser et de hiérarchiser les menaces, les vulnérabilités des systèmes et le patrimoine informationnel à protéger afin de mettre en œuvre une réponse adaptée, sur les plans technique et organisationnel :

– adoption d'une défense en profondeur des systèmes d'information afin de rendre plus difficile la progression des attaquants ;

– développement de capacités de détection et de réaction aux attaques informatiques pour agir rapidement et limiter les dommages ;

– maintien d'un parc informatique sain ;

– sensibilisation et mobilisation de tous les acteurs de l'organisation.

ÉLEVER LE NIVEAU DE SÉCURITÉ DES ORGANISATIONS

Si le projet de réseau interministériel de l'État (RIE) devrait durablement renforcer la résilience des systèmes d'information, le niveau de sécurité informatique des OIV (cf. encadré 3) est loin d'être assuré, encore trop éloigné des préoccupations des dirigeants. Or la sécurité de ces

(41) Les centrifugeuses d'enrichissement en uranium étaient isolées physiquement mais ont été infectées par Stuxnet par des clés USB.
(42) Eudes Y. (2013), "Eugène Kaspersky, M Cybersécurité", *Le Monde*, 10 janvier.

infrastructures est un enjeu de souveraineté nationale, comme le rappelle le président Obama dans un décret du 12 février 2013[43] visant à renforcer la protection des opérateurs. Devant l'ampleur du risque, la réglementation vis-à-vis de ces opérateurs devrait être renforcée avec :

– l'obligation de s'équiper de systèmes de détection d'attaques labellisés : l'obligation de déclarer des attaques n'est pas suffisante puisqu'une attaque non détectée ne peut *de facto* être déclarée ;
– le maintien à jour d'une cartographie des systèmes d'information et des processus industriels critiques ;
– la participation obligatoire, lorsque requise, à des tests de cybersécurité mis en œuvre dans le cadre national (PIRANET) et européen (Cyber Europe) ;
– l'isolation des réseaux traitant de données jugées vitales.

L'ANSSI, quant à elle, devrait être dotée d'un pouvoir de contrôle sur la mise en œuvre de cette réglementation.

PROPOSITION 1

Renforcer les exigences de sécurité imposées aux opérateurs d'importance vitale, sous le contrôle de l'Agence nationale de la sécurité des systèmes d'information.

Les outils méthodologiques classiques de gestion des risques[44] sont complexes à déployer au sein de structures souvent peu matures en termes de sécurité des systèmes d'information et ne sont pas adaptés aux TPE/PME. Il est nécessaire de proposer des approches simples permettant aux TPE/PME d'analyser leurs pratiques informatiques, leur niveau d'exposition aux cyberattaques et les dommages que celles-ci peuvent induire. De tels outils devraient être proposés aux entreprises par l'ANSSI ou le CLUSIF, et mis en œuvre avec l'aide des DIRECCTE[45].

PROPOSITION 2

Développer et mettre à la disposition des petites et moyennes entreprises des outils simples pour gérer les risques.

STRUCTURER L'ÉCOSYSTÈME INDUSTRIEL DE LA CYBERSÉCURITÉ

Un écosystème industriel éclaté, peu valorisant pour les compétences technologiques françaises

La France dispose d'un excellent niveau de recherche académique dans le domaine de la cryptologie[46]. L'expertise en matière de cartes à puces est aussi de renommée mondiale, symbolisée par la réussite de l'entreprise Gemalto (qui a remplacé Alcatel-Lucent dans le CAC 40 en décembre 2012). **Ces succès ne doivent cependant pas cacher le retard technologique et industriel majeur dans de nombreux secteurs clés de la technique informatique** : microprocesseurs, systèmes d'exploitation, équipements de télécommunication, etc.

Malgré un tissu industriel de bonne qualité, emmené par des grands groupes (Bull, Cassidian, Thalès), des PME dynamiques (Netasq)[47] et des projets prometteurs (cf. encadré 4), les entreprises sont généralement fragiles financièrement et ont du mal à atteindre une taille critique nécessaire pour accéder aux marchés internationaux.

Encadré 4

DAVFI – Un antivirus français pour plus de souveraineté

DAVFI (Démonstrateurs d'antivirus français et internationaux), programme de recherche lancé en octobre 2012 et soutenu dans le cadre des "Investissements d'avenir", a pour objectif de commercialiser en 2014 un antivirus à destination des administrations et des OIV, mais aussi des entreprises et des particuliers. Il se base sur les travaux conduits depuis une dizaine d'années par le laboratoire de cryptologie et de virologie opérationnelles de l'ESIEA, école d'ingénieurs qui participe au consortium DAVFI, au même titre que les entreprises Qosmos, Teclib, DCNS et Nov'IT (chef de file du projet). Cet antivirus vise à garantir la souveraineté numérique française et européenne grâce à une approche technique innovante et un code source en grande partie ouvert.

La création en avril 2012 d'un bureau de "Politique industrielle et assistance" au sein de l'ANSSI marque toutefois sa volonté de développer une vision industrielle de la cybersécurité.

(43) *Executive order: Improving critical infrastructure cybersecurity*.
(44) Les plus connus sont la méthode EBIOS développée par l'ANSSI et la norme ISO/IEC 27005 qui fournit les principes à respecter par toute méthode de gestion des risques.
(45) Direction régionale des entreprises, de la concurrence, de la consommation, du travail et de l'emploi.
(46) Science qui a pour but de chiffrer des messages afin de les rendre inintelligibles. Elle englobe deux domaines : la cryptographie (l'écriture secrète) et la cryptanalyse (le déchiffrage).
(47) Qui a été rachetée par Cassidian Cyber security, filiale d'EADS, en octobre 2012.

Des mécanismes de coopération public-privé peu développés

Internet est un environnement extrêmement dynamique dans lequel les technologies, les usages et les marchés évoluent constamment. Il nécessite donc d'être accompagné et régulé par des politiques publiques flexibles. **La coopération public-privé peut constituer un mode d'intervention efficace[48], qui réunit tous les acteurs (entreprises, pouvoirs publics, universitaires, société civile) pour rechercher des solutions pragmatiques bénéficiant à la société dans son ensemble.** La capacité à orienter le secteur privé, à sensibiliser les acteurs économiques et à effectuer un partage d'informations est fondamentale pour élever le niveau général de sécurité. À ce titre, la création en 2011 par le Royaume-Uni d'un *cybersecurity hub* réunissant les dirigeants des plus grosses entreprises britanniques de cinq secteurs stratégiques (défense, télécoms, finance, industrie pharmaceutique et énergie) autour du GCHQ (Government Communications Headquarters, dont dépend la structure équivalente de l'ANSSI) est une initiative intéressante qui impulse une dynamique de coopération.

À l'exception de l'association Signal Spam (cf. encadré 5), on peut reprocher à la France un manque de dialogue et une coopération insuffisante entre les différents acteurs de la sécurité.

Encadré 5

Signal Spam - Seul exemple de partenariat public-privé réussi ?

Signal Spam est une association qui regroupe des organismes publics (CNIL, ANSSI, OCLCTIC, Gendarmerie nationale) et privés (fournisseurs d'accès Internet, expéditeurs de messages, éditeurs de logiciels de sécurité, etc.) dans le but de lutter contre les spams et la cybercriminalité. Pour cela, elle recueille les signalements des internautes grâce à sa plateforme en ligne (www.signal-spam.fr) et les redistribue à ses partenaires sous forme d'information adaptée à leurs différentes missions : "top 30" des plus gros spammeurs en France pour la CNIL, détection d'ordinateurs infectés pour les fournisseurs d'accès et l'ANSSI, etc. L'association est intégralement financée sur fonds privés, car les entreprises trouvent un intérêt économique à y participer. Les projets en cours (rapprochement avec l'association Phishing Initiative, participation au projet européen de "Centre de cyberdéfense avancée"[49]) témoignent de la volonté de Signal Spam d'accroître son influence dans la lutte contre la cybercriminalité.

L'ANSSI doit faire émerger des partenariats (interentreprises, public-privé) à l'échelle nationale et européenne. Des initiatives privées pourraient également être soutenues, par l'ANSSI sur le plan technique, et dans le cadre des investissements d'avenir sur le plan financier (à l'image du projet d'antivirus DAVFI, cf. encadré 4).

PROPOSITION 3

Élargir les missions de l'ANSSI pour accompagner le développement de l'offre française de solutions de cybersécurité.

L'absence d'information quantitative fiable

Selon les fournisseurs de solutions de sécurité[50], le niveau de la menace informatique a augmenté au cours des dernières années. Toutefois, l'hétérogénéité de leurs méthodologies d'évaluation et de leurs estimations, conjuguée au caractère commercial de leur activité, font peser de sérieux doutes sur la qualité et l'objectivité des statistiques qu'ils établissent. De plus, l'élaboration de bases statistiques fiables dans le domaine des cyberattaques se heurte à de nombreux biais[51] :

- il est difficile de distinguer un code malveillant d'un autre, en raison de la possibilité relativement aisée de les dupliquer et d'en créer des variantes ;
- les cyberattaques sont souvent conçues pour rester invisibles le plus longtemps possible ;
- la mesure des attaques dépend de la qualité des systèmes de détection ;
- les entreprises touchées par des attaques informatiques peuvent être réticentes à les révéler.

L'OCDE conduit actuellement des travaux méthodologiques[52] destinés à améliorer la qualité des statistiques relatives à la cybersécurité. L'ANSSI, en liaison avec l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), pourrait lui emboîter le pas et participer à la construction d'indicateurs statistiques fiables et reconnus pour évaluer le niveau de la menace (nombre, origine géographique et typologie des attaques). Les équipes d'intervention d'urgence en informatique (CERT : *Computer Emergency Response Team*) doivent être sollicitées pour partager l'information dont elles disposent. Il serait également intéressant d'avoir accès à des données relatives aux vulnérabilités[53] ainsi qu'à l'évolution du marché industriel de la cybersécurité[54].

(48) OCDE (2012), *Cybersecurity policy making at a turning point*.

(49) http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=325188

(50) Voir par exemple les rapports de McAfee, publiés par Panda Security et Symantec.

(51) ANSSI (2011), *op. cit.*

(52) OCDE (2012), "Improving the evidence base for in-formation security and privacy policies: understanding the opportunities and challenges related to measuring information security, privacy and the protection of children online", *OECD Digital Economy Papers*, No. 214, OECD Publishing.

(53) Nombre de vulnérabilités découvertes, temps moyen entre la découverte d'une vulnérabilité et la publication d'une alerte, etc.

(54) Coût généré par les cyberattaques, dépenses de cybersécurité des entreprises, taille du marché des solutions de sécurité, nombre de formations en sécurité informatique, etc.

Des blocages juridiques dommageables pour la sécurité

Le cadre juridique français crée de nombreux blocages susceptibles d'affecter la sécurité des systèmes d'information :

– la loi Godfrain de 1988[55] réprime les comportements informatiques "agressifs" : appliquée de manière stricte, elle condamne pénalement le fait de divulguer publiquement une faille de sécurité jusque-là inconnue (sécurité par transparence ou *full disclosure*) alors que cela incite les éditeurs de logiciels à concevoir des correctifs ;

– la rétroingénierie, qui consiste à étudier un objet pour en déterminer son fonctionnement interne ou sa méthode de fabrication, est interdite lorsqu'elle est effectuée pour des raisons de sécurité informatique[56]. C'est pourtant le seul moyen d'évaluer le degré de sécurité de produits propriétaires ;

– des mesures techniques de protection[57] d'œuvres numériques peuvent créer des vulnérabilités dans les systèmes d'information. Ainsi, le système de protection XCP installait automatiquement un logiciel contenant des failles de sécurité lors de la lecture d'un CD audio. Or le contournement de ces mesures est interdit par la loi relative au droit d'auteur et aux droits voisins dans la société de l'information (DADVSI, 2006) ;

– les brevets logiciels offrent la possibilité d'obtenir un monopole sur des techniques algorithmiques, y compris lorsque celles-ci sont nécessaires pour assurer la sécurité. L'article 52 de la Convention sur le brevet européen de 1973[58] exclut les "programmes d'ordinateur" du champ des inventions brevetables, mais l'Office européen des brevets (OEB) délivre en pratique des brevets logiciels en raison d'une interprétation extensive de la Convention et d'un modèle économique et de gouvernance discutable.

Les chercheurs en informatique se trouvent dans une situation d'insécurité juridique qui limite leur champ de travail et réduit un vivier de compétences pourtant indispensables pour anticiper, innover et améliorer la sécurité.

S'il ne s'agit pas de remettre en cause le fondement de ces législations, **il conviendrait d'engager une réflexion pour assouplir ce cadre juridique et définir des conditions permettant aux chercheurs de conduire des expérimentations qui mettent en jeu la sécurité des systèmes d'information, dans un cadre juridique et technique clairement défini.**

Des initiatives telles que le Laboratoire de haute sécurité informatique de l'Inria à Nancy pourraient être reproduites : placé dans un environnement fermé avec un réseau isolé et des locaux protégés accessibles par reconnaissance biométrique, il offre un cadre technologique et réglementaire fiable pour mener des expérimentations et manipulations à caractère sensible.

PROPOSITION 4

Revoir le cadre juridique afin de conduire, sous le contrôle de l'ANSSI et d'un comité d'éthique *ad hoc*, des expérimentations sur la sécurité des logiciels et les moyens de traiter les attaques.

CONCLUSION

La France a su développer une recherche académique et des formations d'excellence reconnues au plan international. Toutefois, l'offre de formation est limitée et ne parvient pas à répondre à la demande croissante d'experts en sécurité informatique.
De manière plus générale, la France est confrontée à un véritable déficit d'éducation à l'informatique, qui pourrait être comblé par l'enseignement de l'usage et des langages numériques dès le primaire[59] et le secondaire. Susciter la curiosité des nouvelles générations pour la sécurité informatique est impératif pour élever le niveau de cybersécurité : le gouvernement japonais a par exemple organisé en février 2013 son premier concours de *hacking*, destiné à développer un pôle d'expertise en sécurité informatique.

▶ Mots clés : **cybersécurité, sécurité des systèmes d'information, cyberespionnage, ANSSI, gestion des risques.**

Mars 2013
n° 324
LA NOTE D'ANALYSE

Antton Achiary, Joël Hamelin
et Dominique Auverlot,
département Développement durable.

Les auteurs tiennent à remercier l'ensemble des experts qu'ils ont pu solliciter dans le cadre de ce travail.

(55) Renforcée par la loi pour la confiance dans l'économie numérique (LCEN) de 2004.
(56) Selon l'article L122-6-1 du Code de la propriété intellectuelle, seule la rétroingénierie pour motif d'interopérabilité est autorisée.
(57) MTP, ou en anglais DRM : *digital rights management*.
(58) Cette convention est aussi appelée Convention de Munich.
(59) Interview de Gilles Babinet : "Il faut que nos élèves apprennent à coder dès l'âge de 8 ans", Lepoint.fr, 6 décembre 2012.

DERNIÈRES PUBLICATIONS À CONSULTER

sur www.strategie.gouv.fr, rubrique publications

Notes d'analyse :

N° 323 ■ **Vieillissement et espace urbain. Comment la ville peut-elle accompagner le vieillissement en bonne santé des aînés ?** (février 2013)

N° 322 ■ **Formation professionnelle initiale : l'Allemagne est-elle un modèle pour la France ?** (février 2013)

N° 321 ■ **Gestes de premiers secours : une responsabilité citoyenne** (février 2013)

N° 320 ■ **Comment limiter l'effet rebond des politiques d'efficacité énergétique dans le logement ?** (février 2013)

N° 319 ■ **Pour un affichage environnemental obligatoire des produits de consommation ?** (février 2013)

N° 318 ■ **Quel est l'impact des TIC sur les conditions de travail dans la fonction publique ?** (janvier 2013)

Retrouvez les dernières actualités du Centre d'analyse stratégique sur :

- www.strategie.gouv.fr
- centredanalysestrategique
- @Strategie_Gouv

Centre d'analyse stratégique

La Note d'analyse n° 324 - mars 2013 est une publication du Centre d'analyse stratégique

Directeur de la publication :
Vincent Chriqui, directeur général

Directeur de la rédaction :
Hervé Monange,
directeur général adjoint

Secrétaires de rédaction :
Delphine Gorges
Valérie Senné

Dépôt légal : mars 2013

N° ISSN : 1760-5733

Contact presse :
Jean-Michel Roullé, responsable de la communication
01 42 75 61 37 / 06 46 55 38 38
jean-michel.roulle@strategie.gouv.fr

Le Centre d'analyse stratégique est une institution d'expertise et d'aide à la décision placée auprès du Premier ministre. Il a pour mission d'éclairer le gouvernement dans la définition et la mise en œuvre de ses orientations stratégiques en matière économique, sociale, environnementale et technologique. Il préfigure, à la demande du Premier ministre, les principales réformes gouvernementales. Il mène par ailleurs, de sa propre initiative, des études et analyses dans le cadre d'un programme de travail annuel. Il s'appuie sur un comité d'orientation qui comprend onze membres, dont deux députés et deux sénateurs et un membre du Conseil économique, social et environnemental. Il travaille en réseau avec les principaux conseils d'expertise et de concertation placés auprès du Premier ministre.

www.strategie.gouv.fr