Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

Défis

L'Intelligence stratégique au service de la compétitivité

1

2013

Editorial

Eric DELBECQUE,
Chef du département Sécurité économique

Entretien avec
Claude REVEL,
Déléguée Interministérielle à l'Intelligence Economique

Enjeux

Relevons le défi de la guerre économique
Eric DELBECQUE,
Chef du département Sécurité économique

l'Égide et la plume

Focus
Un nouvel Art de la Guerre, de Jean-François Phélizon, Editions Nuvis, 2013.

L 'actualité éditoriale

Actualités

La rentrée de la 17 ème Session nationale spécialisée

A paraître aux éditions Vuibert

Colloques

Retours de conférences

Dans les médias

Explorer La cybersécurité

Le cybermonde : un enjeu éminemment politique et sociétal
Axelle LEMAIRE, *Députée socialiste pour l'Europe du Nord à l'Assemblée nationale*

La cybersécurité : quel rôle pour les Etats ?
Patrick PAILLOUX, *Directeur général de l'ANSSI*

La cybersécurité : un chantier dont on ne peut plus faire l'économie
Nicolas ARPAGIAN, *Directeur scientifique du cycle « Sécurité Numérique » à l'INHESJ*

Cybersécurité : comment lutter contre une menace technologique qui évolue en permanence
Général Jacques HÉBRARD, *commandant le Pôle judiciaire de la Gendarmerie nationale.*

Prise en compte de la cybersécurité dans les entreprises, quelle est la réalité ?
Anne SOUVIRA, *Commissaire Divisionnaire Chef de la BEFTI*

Quelles sont les contraintes et les réponses des magistrats pour traiter les affaires cybercriminelles ?
Myriam QUÉMÉNER, *Magistrat*

La nationalité d'un prestataire peut-elle faire la différence ?
Etienne DROUARD, *Avocat à la Cour, cabinet K&L Gates, Chargé d'enseignement à l'INHESJ*

Quelle place pour la coopération internationale pour lutter contre la cybercriminalité ?
Thomas CASSUTO, *Magistrat, Docteur en droit*

Entretien avec
Pascal BUFFARD, *Président du Cigref*

Pour aller plus loin
La sécurité des smartphones

A signaler autour du sujet
Bibliographie
Veille Cybersécurité

ÉDITORIAL

Par **ÉRIC DELBECQUE**
Chef du département Sécurité économique de l'INHESJ

DéfIS est la revue trimestrielle du département sécurité économique. Téléchargeable en ligne sur le site de l'INHESJ, elle est également diffusée auprès de ses abonnés.

Mais pourquoi une nouvelle lettre dédiée à l'intelligence économique ? La question mérite d'être posée au regard des nombreux blogs, sites web, lettres dont la qualité informative, et parfois d'analyse, est à saluer. **Celle-ci poursuit plusieurs objectifs : décloisonner, créer du sens et transmettre.**

Décloisonner l'intelligence économique en ouvrant le périmètre du débat. C'est un des premiers défis à relever pour un domaine qui reste encore trop souvent une affaire de spécialistes s'adressant à des spécialistes. Deux rubriques phares, « **Explorer** » et « **Enjeux** », contribuent à alimenter la réflexion sur les enjeux de sûreté des entreprises et d'intelligence économique considérés comme tstratégiques. Une troisième rubrique, « **Entretiens avec… »,** consacrée à des acteurs majeurs dans les dispositifs d'intelligence économique privé et public, combine les approches opérationnelles et les perspectives théoriques. Conçue comme une tribune transdisciplinaire, ouverte à des experts variés, à des pensées innovantes (notamment de jeunes chercheurs, docteurs ou post-doctorants), à des témoignages d'acteurs privés et publics. Cette revue en ligne donne à chacun l'opportunité d'apporter une pierre à l'édifice pour comprendre la portée réelle des événements qui font l'actualité et qui constituent les nouveaux défis de l'intelligence stratégique. La cybersécurité comptent au nombre des problématiques prioritaires : nous avons donc choisi de l'aborder dès le premier numéro. Une rubrique « Actualités » met à disposition des lecteurs l'agenda événementiel et éditorial du Département sécurité économique.

DéfIS manifeste la conviction que l'intelligence économique constitue le dérivé d'une matrice encore plus fondamentale : l'intelligence stratégique. Celle-ci s'impose dorénavant au privé comme au public.

DéfIS assure en outre la transmission de la production éditoriale du département, laquelle forme désormais **un corpus doctrinal indispensable pour comprendre en profondeur l'IE**. La rubrique « **L'*Egide et la plume*** », sélectionne quant à elle les ouvrages éclairant le champ large de l'intelligence stratégique et qui méritent donc d'être commentés ou signalés. Plus généralement, il s'agit de diffuser les résultats du travail quotidien réalisé par le département sécurité économique à l'ensemble de la communauté de l'intelligence économique et, au-delà, à tous ceux que la discipline peut intéresser. La revue nourrit également l'ambition de renforcer et cristalliser les liens entre l'ensemble des partenaires, intervenants, auditeurs et diplômés qui participent à la vie du Département.

Enfin, DéfIS manifeste la conviction que l'intelligence économique constitue le dérivé d'une matrice encore plus fondamentale : l'intelligence stratégique. Celle-ci s'impose dorénavant au privé comme au public. La formule autorise à accepter l'idée que les organisations exigent désormais de nouveaux modes de gouvernance, de pilotage, de management et de « fabrication » de la stratégie qu'elles ne trouveront qu'en assemblant les pièces d'un authentique dispositif interne d'intelligence stratégique dont nous nous proposons d'explorer les possibles et les lignes d'horizon dans les numéros de cette publication. Il y a là, en effet, matière à relever de vrais DéfIS… ■

➔ RETOUR AU SOMMAIRE

Par **Axelle LEMAIRE**
Députée socialiste pour l'Europe du Nord à l'Assemblée nationale

Le cybermonde : un enjeu éminemment politique et sociétal

Le cybermonde ouvre une révolution anthropologique. Tout l'enjeu de la digitalisation de nos sociétés est sans doute là : dans notre aptitude à poser les bonnes questions liées à la dynamique de numérisation qui renouvelle fortement notre vision du monde, le lien entre l'homme et la technique, et notre expérience des rapports humains.

En tout premier lieu, l'Internet pose aujourd'hui la question des libertés individuelles. Si l'affaire Prism constitue un dossier majeur, c'est parce qu'elle a effacé la notion de sphère privée et élargi le travail du renseignement à ce qui ne devrait normalement pas le concerner. A cet égard, la traçabilité absolue des individus sur la Toile – si l'on comprend qu'elle pourrait rester techniquement inévitable – mérite d'être rigoureusement encadrée par la loi afin qu'aucun intérêt politique ou économique n'en fasse une arme de manipulation du citoyen ou du consommateur. La construction d'un régime juridique relatif à l'Identité numérique pourrait en partie répondre à ces préoccupations.

En second lieu, c'est la qualité de notre rapport à l'autre qu'interroge l'usage de la cybersphère, comme peuvent en témoigner en particulier les pratiques sur les réseaux sociaux. Devant ou derrière l'écran d'ordinateur, tout n'est pas permis, et le virtuel produit du réel : chacun a droit au respect de ses droits, et de sa dignité. Attenter à la réputation d'une personne ou dévoiler son espace intime apparaît comme une violation de la vie privée et l'outil virtuel ne rend pas l'offense immatérielle. D'où l'importance de renforcer les protections existantes. Ainsi, le projet de loi pour l'égalité entre les femmes et les hommes modifient ainsi, par exemple, l'article 6 de la loi du 21 juin 2004 relative à la confiance dans l'économie numérique en ajoutant à l'interdiction de la haine raciale, « la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou de leur handicap ».

Ensuite, la montée en puissance des problématiques de cybersécurité rappelle que l'univers numérique n'est pas immunisé contre le crime. Il permet aux marchés porteurs de l'escroquerie, de la falsification, de l'extorsion ou encore de l'usurpation d'identité de trouver de nouveaux espaces de conquêtes. Les citoyens comme les organisations peuvent en être victimes. Les entreprises sont d'autant plus vulnérables qu'elles dépendent de plus en plus des systèmes d'information dans leur fonctionnement, et sont amenés à produire ou traiter des données qui peuvent être utilisée à des fins illicites. La cybersécurité est un bouclier indispensable pour les opérateurs d'importance vitale (OIV). Il est donc impératif que les entreprises se dotent de dispositifs de défense efficients pour lutter contre les cyberattaques, afin de se prémunir contre une rupture de la chaîne de production d'une industrie, ou encore d'une paralysie de fonctionnement d'un Etat. A cet égard, la formation et la sensibilisation des employés aux cybermenaces

est primordiale et des efforts budgétaires sont encore nécessaires. **La France pourrait afficher une certaine exemplarité dans sa capacité à faire émerger une culture de la cybersécurité.** Il y a, en effet, une opportunité historique de créer des emplois et des produits de sécurité en ce domaine, par le développement d'un véritable esprit de filière industrielle qui placerait la France dans le peloton de tête de la compétition internationale. C'est ce que vise notamment le Comité de la filière industrielle de sécurité mis en place le 23 Octobre 2013.

Ce sont enfin les rapports entre les puissances, les nations, les Etats qui subissent l'influence profonde de la digitalisation de notre espace d'action. On va même aujourd'hui jusqu'à parler de « cyberguerre ». Les affrontements entre la Chine et les Etats-Unis s'expriment fréquemment sur le terrain du virtuel, avec pour objet l'acquisition de l'information stratégique. Selon les médias, la Chine, depuis 2006, aurait mobilisé une unité spéciale 61398 pour mener une vaste opération de cyber-espionnage baptisée APT1 (Advanced Persistant Threat 1, menace persistante avancée) contre les Etats-Unis, le Royaume-Uni et le Canada. De son côté, le président américain Barack Obama a désormais la possibilité, depuis février 2013, de lancer des offensives préventives dans le cyberespace dès lors que des preuves solides démontrent l'imminence d'une attaque venant de l'étranger. Ce sont ainsi tous les dispositifs de défense des Etats qui évoluent et s'adaptent au nouvel espace d'affrontement que constitue la cybersphère.

La France pourrait afficher une certaine exemplarité dans sa capacité à faire émerger une culture de la cybersécurité.

Dans ce contexte, la France doit aussi s'adapter. Dans le rapport Bockel du 18 juillet 2012, la cyberdéfense et la protection des systèmes d'information sont élevées au rang de priorité nationale. Pour la première fois, le livre blanc sur la défense fait deux références aux objectifs militaires de cybersécurité : notamment en renforçant la protection des systèmes d'information des opérateurs publics et privés et en développant des capacités de cyberdéfense militaire. La Loi de Programmation Militaire 2014-2019, votée le 21 octobre dernier ajoute un article L. 2321-2 au Code de la défense, permettant à l'ANSSI d'étudier l'action d'un logiciel malveillant ou d'accéder à un serveur informatique à l'origine d'une attaque, une demande de longue date émanant des services de l'Etat. Et dans un contexte budgétaire pourtant tendu, la loi prévoit le renforcement des effectifs dédiés au renseignement, à la cyberdéfense et aux Forces spéciales, avec 1000 emplois supplémentaires. Le Président de la République a utilisé des mots forts pour résumer cette volonté au sommet de l'Etat, la France est entrée dans une guerre économique. La cybersécurité est un des éléments d'action.

L'Union Européenne se mobilise également sur cette problématique. Les attaques subies par l'Estonie et le Danemark ont réveillé les consciences. La Commission européenne et le Service européen pour l'action extérieure (SEAE) ont défini une stratégie visant à garantir « un cyberespace ouvert, sûr et sécurisé ». Le Parlement européen et le Conseil de l'Europe ont, quant à eux, publié une proposition de directive (COM(2013) 48 final), en février dernier, visant à renforcer la sécurité des réseaux et de l'information des Etats membres. Ces initiatives témoignent d'une volonté politique de coopérer en matière de cybersécurité.

Si l'ensemble de ces mesures visent en premier lieu à sécuriser le cyberespace, elles ont surtout pour objectif final de restaurer un « espace de confiance pour nos entreprises et nos citoyens »[1] comme l'a appelé de ses vœux Madame la Ministre déléguée chargée des PME, de l'Innovation et de l'Économie numérique, Fleur Pellerin, le jeudi 23 octobre 2013, au cours *des premières rencontres parlementaires de la cybersécurité*. La Ministre a également déclaré : « notre responsabilité est de faire en sorte que le numérique respecte nos valeurs et soit un progrès pour l'ensemble de nos concitoyens »[2].

Pour rester une terre de promesses, le monde numérique doit absolument faire l'objet d'une régulation visant à concilier des intérêts, des impératifs d'adaptabilité et des enjeux de puissance avec le respect des libertés individuelles qui détermineront le visage du cyber-futur qui nous appartient tous. ■

(1) Les premières rencontres parlementaires ont été organisées par Défense et stratégie à Issy-les-Moulineaux (Hauts-de-Seine) le 23 octobre 2013.

(2) Idem.

Par **Patrick PAILLOUX,**
Directeur général de l'ANSSI

Cybersécurité : quel rôle pour les Etats ?

Lorsqu' internet entamait sa conquête du monde, il y a vingt ans, quelques années après la chute du mur de Berlin, il était question de la fin de l'Histoire et de la disparition des États qui seraient devenus inutiles, dans un monde rêvé en route vers la démocratie et soutenu par une économie qui aurait raison de tous les dogmatismes…

Vingt après, force est de constater que cette utopie ne s'est pas matérialisée. Si le cyberespace a imprégné nos vies personnelles et professionnelles, s'il porte le fonctionnement de nos sociétés, notre économie et notre confort, les États sont bien présents dans cet espace à côté d'autres acteurs.

Cette présence des États dans le cyberespace est-elle nécessaire ? Oui, pour au moins trois raisons.

La première est technologique et économique. Les technologies numériques innervent tous les secteurs d'activité au point d'en recomposer certains au risque de leur disparition – commerce en général et distribution de produits culturels en particulier, dopent nos économies jusqu'à l'irrationnel – bulles financières, survalorisation d'entreprises ou de rémunérations, et représentent une part chaque année plus importante de notre croissance. Les États se doivent d'appuyer cette croissance en soutenant la recherche, l'innovation et le développement des jeunes pousses du numérique comme en accompagnant les secteurs en difficulté.

La deuxième raison est fonctionnelle. Les technologies numériques sont au cœur du fonctionnement de nos sociétés. Les transports, les hôpitaux, les banques, la production et la distribution d'énergie ou d'eau potable, les télécommunications, et une grande part du fonctionnement de l'État – des prestations sociales aux systèmes d'armes en passant par le bracelet électronique du prisonnier, sont dépendants de technologies numériques toujours plus imbriquées avec le monde matériel.

Cette dépendance accentue la troisième raison de la nécessaire présence des États dans le cyberespace : l'impérieuse nécessité d'assurer la sécurité – la cybersécurité de nos compatriotes et la défense des intérêts de la France dans un espace sensiblement différent des milieux dans lesquels évoluent les États depuis des siècles.

Mais qu'entend-on au juste par cybersécurité ? La définition donnée en 2011 dans la version publique de la stratégie nationale de sécurité et de défense des systèmes d'information présente la cybersécurité comme un état à atteindre – comme l'est la sécurité routière.

Pour atteindre cet état, trois domaines doivent être pris en compte :

les principes et technologies liés à *la sécurité des systèmes d'information*, de la cryptologie aux règles d'hygiène informatique en passant pas la sécurité des composants électroniques, par une architecture réfléchie des systèmes d'information ou le soutien au développement d'une industrie nationale nécessaire à la disponibilité d'une offre « de confiance » ;

la lutte contre la cybercriminalité, le cyberespace étant devenu un nouveau domaine de développement de la criminalité individuelle et organisée, dans lequel se retrouvent appliquées au monde immatériel des pratiques communes de l'atteinte aux personnes, vol d'identité ou de données bancaires, escroqueries à la vente, harcèlement- aux atteintes aux biens ou à l'image d'institutions ou d'entreprises – défacements, contrefaçons, rumeurs, aux conséquences parfois mortelles ;

la cyberdéfense, c'est-à-dire la protection active des systèmes d'information critiques de la nation qui soutiennent la vie de nos concitoyens, notre développement économique ou nos capacités de défense. Il s'agit alors de lutter contre trois types de menaces :

1. l'espionnage, facilité par la masse d'informations accessibles au travers des réseaux connectés des entreprises, des laboratoires de recherche ou des administrations ;
2. la déstabilisation par la divulgation d'informations destinées à rester confidentielles, la tentative de rendre des services indisponibles ou l'insertion de messages de propagande ;
3. le sabotage, par la modification du fonctionnement ou la destruction d'équipements industriels.

En matière de cybersécurité, c'est donc dans ces trois domaines que doit se déployer l'action de l'État.

Après l'attaque informatique contre l'Estonie, le Livre blanc sur la défense et la sécurité nationale de 2008 a montré que les pouvoirs publics ont pris en compte les enjeux de défense et de sécurité liés au cyberespace.

Aujourd'hui ces technologies appuient une criminalité « ordinaire », demain elles pourraient, par des attaques menées contre nos systèmes d'information, être au service de nouvelles formes d'extorsion ou de terrorisme à grande échelle

L'Agence pour la sécurité des systèmes d'information (ANSSI), créée l'année suivante, anime une organisation transversale qui s'appuie sur l'ensemble des ministères et particulièrement sur les ministères de l'intérieur et de la défense. Dans un contexte budgétaire difficile, elle voit ses effectifs croître, passant d'une centaine d'ingénieurs en 2009 à 350 cette année. Une croissance qui s'explique par l'ampleur de la tâche à accomplir, tant les systèmes d'information de l'État et des opérateurs nationaux les plus critiques sont vulnérables et attaqués, aujourd'hui à des fins d'espionnage. L'ANSSI a la double mission de sécurité des systèmes d'information qui s'appuie notamment sur les compétences des experts en cryptologie, métier d'origine de l'administration dont a été tirée l'agence, mais également sur celles de spécialistes des nombreux domaines des technologies du numérique, et une mission de défense des systèmes d'information qui a vu se développer de nouveaux métiers, notamment ceux liés au traitement des attaques informatiques de grande ampleur.

Les ministres de la justice et de l'intérieur ont, pour leur part, la charge de la lutte contre la cybercriminalité. Du vol de données personnelles au vol d'identité, de la lutte contre la pédopornographie ou l'incitation à la haine à celle menée contre toutes sortes de trafics, de la lutte contre le crime organisée à celle menée contre le terrorisme, ces ministères ont dû s'adapter à l'utilisation des technologies du numérique par les délinquants et criminels. **Aujourd'hui ces technologies appuient une criminalité « ordinaire », demain elles pourraient, par des attaques menées contre nos systèmes d'information, être au service de nouvelles formes d'extorsion ou de terrorisme à grande échelle.** Les conclusions de la mission en cours, confiée au procureur général Marc Robert par ses ministres et celle en charge des petites et moyennes entreprises, de l'innovation et de l'économie numérique devrait permettre d'optimiser l'intégration de ces ministères dans le dispositif national.

Publié en avril 2013, le Livre blanc sur la défense et la sécurité nationale a confirmé l'importance du rôle de l'État dans le domaine de la cybersécurité. Prenant acte de l'ampleur des menaces et des perspectives sombres qu'elles ouvrent en matière de terrorisme, le Livre blanc a annoncé une régulation des pratiques des opérateurs d'importance vitale en matière de sécurité des systèmes d'information. Ainsi, la loi de programmation militaire porte des dispositions visant à renforcer la sécurité de ces opérateurs par l'imposition de règles techniques adaptées au secteur d'activité de l'opérateur, par l'obligation de déclaration d'incidents intervenants sur leurs systèmes d'information les plus critiques et par la capacité d'effectuer des contrôles de la mise en œuvre des règles techniques définies ou des audits de sécurité.

Cette présentation succincte de ce que sont la cybersécurité, les menaces auxquelles nous sommes confrontées dans le cyberespace et l'organisation de la France en ce domaine, illustre la plupart des rôles des États dans le cyberespace en matière de cybersécurité.

Pour compléter ce panorama, il est nécessaire d'évoquer quatre domaines dans lesquels l'État s'implique également, par l'action de l'ensemble des administrations :

- ***l'anticipation des opportunités et des risques* portés par le cyberespace**, notamment par le soutien à la recherche et le développement d'une politique industrielle adaptée. Les perspectives d'un « internet des objets » et de la généralisation des « systèmes embarqués » offrent une chance à notre industrie mais représentent un réel défi en matière de cybersécurité ;

- ***la formation des compétences nécessaires.*** Aujourd'hui l'offre disponible ne suffit pas à combler une demande en forte croissance de personnes formées dans les multiples disciplines de la sécurité des technologies du numérique, à tous niveaux de formation ;

- ***les relations internationales* :** les sujets liés au numérique sont désormais abordés par la plupart des organismes internationaux – Organisation des nations unies (ONU) et ses ramifications, Union européenne, organisation du traité de l'Atlantique nord (OTAN), OCDE, OSCE, G20, etc. Les domaines d'expertise nécessaires vont de la gouvernance d'Internet au droit international des conflits ou à la question des normes, notamment techniques. Les relations bilatérales se révèlent quant à elles cruciales, notamment d'un point de vue opérationnel ;

- ***la sensibilisation et l'information* :** un état de cybersécurité impliquerait que l'ensemble de nos compatriotes soit conscient des enjeux liés au cyberespace et de l'importance d'un comportement responsable en ce domaine. Par exemple par le respect d'un certain nombre de règles d'hygiène informatique. C'est sans doute dans ce domaine que la marge de progression est la plus forte.

Les États ont cependant un rôle particulier dans cet espace qui est à la fois et simultanément un espace universel et de souveraineté.

Pour que le cyberespace soit un espace source d'innovation, de nouveaux usages favorisant l'épanouissement de ceux qui y ont accès, et un vecteur de croissance pour les entreprises comme pour les sociétés, nous devons collectivement travailler à la cybersécurité. **Les États ont cependant un rôle particulier dans cet espace qui est à la fois et simultanément un espace universel et de souveraineté.** La France a choisi une organisation qui permet de prendre en compte l'ensemble des facteurs générateurs de cybersécurité. **L'avenir en ce domaine dépendra de nos choix collectifs pour donner aux administrations compétentes les moyens nécessaires et de choix individuels pour disposer demain des femmes et des hommes qui travaillent, au quotidien, à la cybersécurité.** ■

Par **Nicolas ARPAGIAN**
Directeur scientifique du cycle « Sécurité Numérique » de l'INHESJ

La cybersécurité : un chantier dont on ne peut plus faire l'économie

L'omniprésence des systèmes d'information dans les organisations économiques, administratives et militaires oblige à généraliser la prise en charge de la cybersécurité. Qu'il s'agisse de protéger les infrastructures techniques mais aussi les données numérisées.

L'affaire *WikiLeaks* a montré à la face du monde comment un individu isolé pouvait à l'aide de quelques CD's enregistrables mettre en difficulté le gouvernement d'une hyperpuissance. Il a suffi à un soldat quelques minutes pour transférer, sans savoir-faire technique, des volumes considérables de données stratégiques. Cette affaire illustre les différentes facettes qui font la spécificité de la problématique de la cybersécurité.

Gardons constamment à l'esprit que cette cybersécurité concerne bel et bien deux dimensions, chacune d'une même importance.

D'une part, il s'agit de la sécurité des systèmes d'information : connexions informatiques, téléphoniques, liaisons Wi-Fi ou *bluetooth*, câbles sous-marins et autres communications satellitaires. Ces « voies de circulation » peuvent faire l'objet d'interception, d'altération voire d'interruption. Des Etats, des entreprises et des personnes physiques peuvent être amenés à conduire de telles opérations avec des motivations diverses. Politiques de sécurité, espionnage économique, lutte contre le terrorisme, curiosité malsaine, intention de nuire... la palette des raisons invoquées est extrêmement large. Bien sûr, sauf pour les Etats qui ont légiféré pour encadrer les interventions sur ces équipements par leurs propres services de sécurité ou de police, de tels actes sont *a priori* illicites quand ils sont commis par des officines privées ou des particuliers.

> L'énoncé de ces possibles menaces suffit à comprendre que la cybersécurité est bien une composante essentielle de la sécurité globale.

D'autre part, il s'agit de la sécurité des données au sens large. L'information nourrit de plus en plus l'économie. Et la création de richesses passe plus que jamais par une valorisation notamment via l'apport d'informations. En janvier 2013, un message d'alerte émanant d'un faux compte *Twitter* créé pour l'occasion a permis de faire chuter de 25 % le cours de la compagnie *Audience*, côtée au Nasdaq. Le coût d'une telle manipulation est évidemment dérisoire par rapport au gain ou aux dégâts causés à l'image de marque de la société. Idem dans le cas de campagnes de dénigrement à partir de forums de consommateurs ou de messages mensongers publiés sur le Net. Bien indexés ce sont ces commentaires qui composeront (négativement) la e-réputation de l'entité ciblée.

Le phénomène peut être amplifié à grande échelle si les informations délibérément erronées sont publiées et diffusées via les plateformes de réseaux sociaux. Enfin la confidentialité des données doit également être assurée afin d'en garantir l'intégrité. Pour préserver le patrimoine immatériel qui fait la valeur de l'entreprise. Et participe à sa pérennité.

➔ RETOUR AU SOMMAIRE

L'énoncé de ces possibles menaces suffit à comprendre que la cybersécurité est bien une composante essentielle de la sécurité globale. Et dès lors qu'elle peut affecter le patrimoine économique des entreprises et donc l'avenir de celles-ci et de leurs collaborateurs, constituer un support pour des atteintes aux biens et aux personnes par des mises en danger ou des mises en cause indues, **la cybersécurité est un chantier majeur.**

La notion de chantier, donc d'activité en construction, est intéressante à conserver à l'esprit. Puisque les technologies évoluent sans cesse, les consommateurs s'approprient constamment de nouvelles manières d'employer ces outils et ces services, tandis que des acteurs économiques naissent, fusionnent ou disparaissent au gré de stratégies de firmes planétaires… Bref, cet écosystème est en mutation permanente. Avec l'apparition de nouveaux prestataires et un public de clients/utilisateurs qui s'élargit à grande vitesse. **La cybersécurité se caractérise par quelques traits qui font sa singularité :**

La notion de chantier, donc d'activité en construction, est intéressante à conserver à l'esprit.

- **Un espace d'affrontement asymétrique.** Ici les moyens financiers, humains ou techniques ne sont pas un critère essentiel. Et une personne ayant accès de manière autorisée ou non à des fichiers sensibles peut causer des dommages très conséquents. Il ne s'agit pas d'une guerre de tranchées où seules comptes les troupes que l'on peut aligner face à l'adversaire. Ici il est question d'intelligence, d'adaptation au terrain, de connaissance des modes d'organisation et de fonctionnement de la cible…

- **L'information peut primer sur la puissance accumulée.** En lisant une simple clé USB opportunément garnie, votre compétiteur peut accéder aux conclusions qui ont exigé de votre part des mois, voire des années d'investissement en Recherche et Développement ainsi que des budgets dépensés en millions d'euros. S'il accède à vos données, il peut rattraper sans délai ce qui en temps normal constitue l'élément différenciateur majeur entre des concurrents : le temps. Un processus de fabrication, un plan de développement, une maquette de prototype… toute cette matière grise qui permet à des entreprises d'acquérir et de conserver leur leadership sont potentiellement stockables et donc duplicables sur des supports mobiles.

- **L'émergence d'une société de l'information avec ces propres organes de production.** Dans le cas de WikiLeaks, un simple site Internet a permis de diffuser les télégrammes diplomatiques étatsuniens. La duplication de ces contenus sur d'autres sites a contribué à faire se propager l'information, rendant son effacement illusoire. C'est la même démarche quand des groupes minoritaires d'activistes ouvrent des pages Facebook ou Youtube pour faire entendre leurs opinions. Le *modus operandi* est simplissime, gratuit et assure une exposition optimale. C'est alors que peut débuter une version numérique, et donc à l'échelle mondiale, de « jeu » de gendarmes contre voleurs pour tenter d'identifier et de faire fermer ces sites. Qui mettent ensuite quelques minutes à réapparaitre chez un autre hébergeur sous une identité quasi identique. La viralité de l'information avec l'élaboration de *mailing list* et de forums dédiés favorise spontanément ceux qui cherchent à faire circuler les fichiers. Les moyens d'action à mettre en œuvre pour stopper leur diffusion sont sans commune mesure avec les quelques secondes qu'il suffit pour mettre en ligne une vidéo ou la transférer sur un serveur à des milliers de kilomètres de là.

- **Un cadre juridique encore largement inadapté.** Et qui lèse donc les victimes. En effet, les Etats sont extrêmement réticents – au-delà des discours politiques – à renoncer à exercer leur souveraineté sur leur Internet national. Alors que des prestataires offrent des hébergements informatiques à travers le monde pour quelques euros, les procédures judiciaires sont encore dépendantes de la coopération judiciaire internationale. Cela crée des surcoûts et des pesanteurs qui limitent l'efficacité de la poursuite contre les criminels. Et dissuaderait presque les victimes de porter plainte.

  D'un point de vue institutionnel, la mainmise des Etats-Unis sur les instances de gouvernance d'Internet comme l'*Icann* (www.icann.org) est encore très marquée. Malgré les annonces régulières d'élargissement et de multiplication des organes de décision.

- **Un théâtre d'ombres très peu tenté par la lumière.** En 2013 l'affaire « Prism » a montré comment les Etats-Unis sollicitaient de manière intense les services d'entreprises privées à l'insu des clients de celles-ci. Cette affaire a levé une partie du voile sur certaines pratiques. Dans ce champ d'affrontements numériques, tous les coups sont

permis. Et chacun s'appuie sur ses propres forces : les liens étroits avec le secteur privé en font partie. Et dès lors que la mise à disposition d'informations numérisées peut s'effectuer de manière indolore pour la personne ou l'institution écoutée, pourquoi se priveraient-ils ? Car peu ou prou on constate que les gouvernements ont désormais tous intégré la dimension cybernétique de la sécurité nationale. Qu'il s'agisse d'assurer la défense de leurs intérêts militaires mais également économiques et diplomatiques. Et à ce jeu, la principale faute reste de se faire prendre.

- **Des acteurs économiques aux moyens sans limite.** Dans cet univers d'Internet, les poids lourds de cette économie numérique sont des firmes dont l'existence se compte en quelques années : Alibaba, EBay, Facebook, Google, Huawei, LinkedIn, Twitter ou Yahoo.... Pourtant la plupart d'entre elles ont conquis des clientèles dans le monde entier. Et disposent de capacités financières qui assimilent leurs investissements à des budgets relevant autrefois de la puissance étatique. Ces firmes créent des usages et occupent des marchés qui leur permettent d'asseoir leur leadership de manière pérenne. Celui qui songe à bousculer Google sur l'activité du moteur de recherche devrait aujourd'hui mobiliser des moyens considérables. Même Microsoft, pourtant richement doté et expert es-informatique, peine avec Bing.com à rivaliser avec la jeune pousse fondée en 1998. Ces sociétés sont aujourd'hui des parties prenantes de premier ordre dans la géopolitique d'Internet. Et peuvent agir le cas échéant en harmonie avec les stratégies des Etats. Ces attelages, qui combinent la puissance économique et le savoir-faire technique aux leviers diplomatiques, sont d'une puissance opérationnelle sans égal.

- **L'indolence et la pesanteur des organisations : des freins à la cybersécurité.** Les mesures de sécurité, que l'on parle de sûreté physique ou de protéger des équipements informatiques, sont presque toujours vécues comme des pesanteurs. Qui freinent les échanges, compliquent les communications et dans une certaine mesure pénalisent donc les affaires. La cybersécurité avec ses invitations à ne pas utiliser de connexion wi-fi ouvertes, à préférer les communications cryptées et à éviter les supports mobiles comme les clés USB, peut donc apparaître à contre-courant. Mettre en place des procédures sécurisées et s'y tenir est contraignant. Choisir ses prestataires en fonction de ces critères de sécurité signifie que l'on ne va pas forcément retenir le moins cher ou celui qui propose l'interface la plus fluide. La prise en compte de telles options exige une réelle conviction dans l'efficacité d'un dispositif de sécurité mais aussi une capacité à imposer ses vues aux tenants de la seule approche comptable. Or avoir la capacité de convaincre, de se faire entendre de sa hiérarchie, suppose de se doter d'une vision stratégique qui va bien au-delà d'une approche court-termiste d'économie immédiate. La valorisation de ce qui constitue le patrimoine informationnel de l'entreprise devrait relever d'une volonté partagée au sein des plus hautes sphères de l'organisation. Combien sont-ils/elles à défendre cet axe ? Surtout s'il s'avère qu'il faut changer de fournisseurs en cours d'année car celui originellement retenu n'apporte pas toutes les garanties de fiabilité. Qui assumera le transfert à un autre prestataire avec les dépenses nouvelles générées au nom du maintien de la sécurité de l'information ? Pour une large part des décideurs, ne rien faire et ne rien changer constituera sans doute la recommandation la plus sage. En attendant leur changement de poste ou leur départ pour un autre employeur, l'évaluation des dégâts causés par cette inertie sera au programme des activités de... leur successeur. De quoi s'interroger sur une vision de l'entreprise sur la durée. Donc au-delà du cycle budgétaire trimestriel.

On le comprend aisément la cybersécurité n'est pas qu'une affaire de choix informatiques. Elle affecte les orientations économiques et techniques de l'entreprise/ administration, n'existe pas sans une forte implication du management et exige une attention continue.

On le comprend aisément la cybersécurité n'est pas qu'une affaire de choix informatiques. Elle affecte les orientations économiques et techniques de l'entreprise/administration, n'existe pas sans une forte implication du management et exige une attention continue. Dès lors qu'il faut intégrer les nouveaux outils au fur et à mesure que les collaborateurs se les approprient afin d'en encadrer les risques. Et donc établir une véritable stratégie de cybersécurité afin de déterminer ce que l'on souhaite protéger et les moyens que l'on est prêt à y consacrer. Un exercice salutaire qui sera l'occasion de réfléchir à ce qui constitue les actifs stratégiques de l'entreprise. Et à la manière dont ils sont valorisés. ■

Par **Général Jacques HÉBRARD**
Commandant le Pôle judiciaire de la Gendarmerie nationale.

Cybersécurité : Comment lutter contre une menace technologique qui évolue en permanence ?

Selon le philosophe Michel Serre, « c'est lorsqu'interviennent des révolutions concernant l'information que les civilisations basculent et se mettent en place de manière nouvelle ». La révolution du numérique et la forte croissance d'Internet au milieu des années 90 ont légitimement donné naissance à de nouvelles menaces regroupées dans le concept de cybercriminalité. Il fallait donc que l'action des services de sécurité réagisse au plus vite au « technocrime » et cerne la réalité de ce phénomène. Vingt ans après, alors que tous les experts s'accordent à reconnaître l'utilisation massive des technologies numériques dans la commission des infractions, le concept de cybersécurité est bien en place au sein de la gendarmerie. Il s'appuie sur la volonté de l'institution de travailler sur l'ensemble du spectre de la menace, à savoir la prévention, la répression et la prospective, ces trois composantes étant foncièrement interdépendantes.

Au fil des années, nos sociétés sont devenues entièrement dépendantes des technologies de l'information et de la communication. Ainsi, selon le site journaldunet.com, la France comptait près de 48 millions d'internautes en janvier 2013, soit quasiment 3 français sur 4. Du fait de cette explosion, on est passé depuis de nombreuses années de l'atteinte aux ordinateurs à l'atteinte aux réseaux. Les actes de délinquance numérique se sont diversifiés, mais, encore de nos jours, ceux-ci sont rarement spécifiques et concernent plutôt des délits classiques qui ont développé de nouveaux modes d'action, comme par exemple l'escroquerie sous toutes ses formes, dorénavant omniprésente sur Internet. Sphère privée, entreprises et états : rien ni personne n'est à l'abri. La menace se glisse même jusque dans nos voitures, où l'électronique a remplacé la mécanique et le garagiste ne peut plus rien faire sans sa valise de diagnostic. Sans parler des menaces pesant sur nos moyens de paiement ou nos pièces d'identité et autres documents officiels, toujours plus sécurisés mais pour lesquels le « criminel technologique » trouve toujours la faille.

Les efforts de la gendarmerie pour répondre à l'avènement de la délinquance informatique sous toutes ses formes ont été constants dès la découverte du phénomène. On peut noter, entre autres étapes marquantes de cette évolution : l'introduction d'une dimension informatique dans les attributions des enquêteurs en matière de délinquance économique et financière (DEFI) dès le début des années 90, la création du département informatique électronique (INL) à l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN) en 1992, la création d'une division de lutte contre la cybercriminalité (DLCC) au Service technique de recherches judiciaires et de documentation (STRJD) en 2006 et plus récemment la création d'un Plateau d'investigation cybercriminalité et analyses numériques (PICyAN) en 2012 au sein du Pôle judiciaire de la gendarmerie nationale

(1) Le PJGN regroupe sous un commandement unique l'IRCGN et le STRJD, afin d'assurer une cohérence globale dans la réponse opérationnelle judiciaire au niveau central.

(PJGN) [1]. Poursuivant la logique de prise en compte globale de la menace, ce plateau a pour principal objectif de favoriser les synergies entre experts judiciaires de l'IRCGN et enquêteurs spécialisés de la DLCC, en lien avec la communauté des enquêteurs en nouvelle technologie numérique (N-TECH) [2] présents sur l'ensemble du territoire.

Face au développement exponentiel de la société de l'information (nomadisme, réseaux sociaux, banque en ligne, paiement mobile...) et à l'essor d'une cybercriminalité ingénieuse, il est primordial que des efforts soient conduits afin de convaincre de l'importance et de l'enjeu de la cybersécurité. La gendarmerie intègre systématiquement la problématique de la cybersécurité dans les actions de sensibilisation qu'elle conduit auprès des établissements scolaires (par les brigades de prévention de la délinquance juvénile ou les unités territoriales), des professionnels (par le biais du réseau des référents Intelligence économique) et des seniors (par les unités territoriales). Ce dispositif repose essentiellement sur le niveau d'implication des intervenants dans cette nouvelle mission, connexe à leur activité principale.

La loi sur la prévention de la délinquance de mars 2007 et la loi d'orientation et de programmation pour la performance de la sécurité intérieure de mars 2011 ont introduit de nouveaux moyens d'enquête adaptés à la cybercriminalité au profit des services de police et de gendarmerie. Le corpus juridique français est d'ailleurs particulièrement riche et la loi française a souvent été novatrice en l'espèce (loi informatique et des libertés dès 1978 ou loi Godfrain en matière d'attaques contre les systèmes informatiques en 1998). Cependant, l'adaptation de certains moyens d'enquêtes aux évolutions technologiques de la cybercriminalité demeure en permanence recherchée et sollicitée auprès du législateur. Ainsi, les cyberpatrouilleurs qui recherchent quotidiennement les infractions liées à la pédopornographie doivent voir leur champ d'intervention étendu à bien d'autres infractions présentes sur le net (incitation à la haine, vente illégale de tout type de produit,...). Il en va de même d'ailleurs pour les enquêtes sous pseudonyme.

La définition des actes techniques qu'il est possible de réaliser en matière de cybercriminalité doit également évoluer. Ainsi, la tendance actuelle du cloud-computing, qui consiste à ne plus laisser ses données sur son poste informatique mais sur un ensemble de machine appartenant à ce nuage, doit inciter le législateur à repenser le concept de perquisition tel que défini par l'article 57-1 du CPP. Il s'agit ni plus ni moins que d'envisager le concept de cyberperquisition, tout en respectant les termes de la convention de Budapest sur la cybercriminalité.

Signalons enfin l'existence de plus en plus répandue de techniques cryptographiques, utilisées initialement pour sécuriser des transactions ou les communications sur les réseaux, qui sont de plus en plus souvent intégrées aux systèmes d'exploitation (ex : Bitlocker depuis Microsoft Vista) ou nativement dans les disques durs auto-chiffrants ou encore les téléphones portables (smartphones). Il est donc probable que l'analyse forensique en laboratoire, portant sur un objet saisi, placé sous scellé, déconnecté du réseau, va devoir s'adapter et se tourner vers ce type d' analyse sur « machine vivante » autrement dit le live-forensics.

Enfin, si l'on veut être efficace dans la lutte contre la cybercriminalité, il faut pouvoir connaître précisément l'étendue de tout phénomène détecté localement et donc pouvoir recevoir et traiter un maximum d'informations de la part des victimes ou de partenaires publics/privés. Ceux-ci faisant de plus en plus de veille sur les menaces qui touchent les réseaux informatiques, et ce bien évidemment en provenance du monde entier. C'est la finalité des différentes coopérations européennes, voire internationales, qui se développent sans cesse. Citons par exemple l'EC3 (European Cybercrime Center) créé en janvier 2013, dont l'objet est de concentrer en une même unité tous les efforts développés par Europol en matière de cybercriminalité.

« L'homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique » disait Albert Einstein. Dans cette révolution technologique que constitue l'avènement du numérique, la lutte contre la cybercriminalité doit donc bien être notre préoccupation essentielle, et la composante majeure d'une politique de défense et de sécurité des personnes, des entreprises et des états. La cybersécurité se gagne ainsi par une approche globale pro-active répondant à des défis de trois ordres : juridique, technique et culturel.

(2) Opérationnel depuis 2003, le réseau N-TECH représente aujourd'hui une communauté de près de 1000 gendarmes spécialisés et formés qui assurent, sur l'ensemble du territoire où la gendarmerie exerce sa compétence, une activité de lutte contre la cybercriminalité.

➔ RETOUR AU SOMMAIRE

Par **Anne SOUVIRA**
Commissaire Divisionnaire
Chef de la BEFTI [1]

Prise en **compte** de la **cybersécurité** dans les **entreprises**, quelle est la **réalité ?**

Une étude, privilégiant l'approche opérationnelle a été réalisée sur la base des retours d'expérience de la Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information (BEFTI) compétente sur Paris et ses trois départements limitrophes, soit l'essentiel des états-majors des firmes en France. Les Responsables de la Sécurité des Systèmes d'Information commencent à bien convaincre leurs Directions à dialoguer avec les comex, et à mettre en place le cas échéant des cellules de réaction de crise. Cela vaut surtout pour les grandes entreprises, mais pas toutes, certaines d'entre elles résistent encore. Ces dernières n'échappent pas aux attaques sournoises persistantes qu'elles n'ont pas su prévenir. Si le discours visant à alerter des risques de cyberattaques a suscité la prise de conscience de la part de quelques décideurs, sa portée n'atteint pas encore la place publique et se limite encore trop au microcosme du cybermonde.

Pour les petites et moyennes entreprises la prise en compte de la menace passe d'abord par une amélioration de la culture de sécurité informatique qu'il faut élever significativement, plus que par des investissements en produits coûteux. Il leur faut également procéder à une meilleure identification de la menace. En élevant notamment le niveau de connaissance sur les obligations de l'entreprise vis-à-vis des données à caractère personnel (DCP), des vulnérabilités du réseau informatique ou téléphonique, des failles techniques. Mais il convient aussi d'avoir recours à des outils juridiques appropriés pour mieux appréhender et répondre de façon adaptée aux cyberattaques. Cela commence par exemple par un contrat de maintenance intégrant les conditions de récupération de données en cas de crise, la sauvegarde quotidienne des journaux de connexions, un plan de continuité d'activité, une charte informatique qui permet à l'employeur et ses personnels de travailler dans la loyauté informatique... Ce sont autant de mesures qui devraient être systématisées au sein des organisations, quels que soit leur taille et leur secteur d'activité. Nous savons pourtant que les TPE-PME ne sont pas armées comme les grandes entreprises, sauf exceptions, alors que les dégâts sont tout aussi dévastateurs en termes de perte de chiffre d'affaires et d'emplois.

Mais c'est encore la nécessité du moment qui fait loi, celle qui pousse à faire des économies de bout de chandelle et à ne pas lever la tête des urgences du quotidien et qui conduit à faire la politique de l'autruche. Les mises à jour des systèmes d›information (SI) représentent un coût et ne sont pas souvent intégrées dans le contrat de maintenance. Les SI infogérés à distance sont insuffisamment contrôlés et la tendance de recourir à de « petites boîtes » réputées moins chères reste trop courante. Ces dernières, débordées par l'augmentation de la demande, ne respectent pas toujours les règles de sécurité, notamment dans la téléphonie. Or ces petites impasses s'avèrent être de mauvais calculs à long terme, ainsi les lignes de télégestion qui ne requièrent pas le niveau de protection qu'il convient et avec des codes triviaux qui restent inchangés sont des incitations aux tentatives d'actes de malveillance et d'escroquerie.

(1) La BEFTI est une des 7 Brigades spécialisées de la Sous-Direction des Affaires Economiques et Financières de la Direction Régionale de la Police Judiciaire de la préfecture de Police

Les principales attaques constatées

Les attaques qui sont portées à la connaissance des forces de sécurité et parfois médiatisées par l'entreprise, se répartissent entre **les entraves à son activité** (dénis de services) en vue d'une prise d'avantage concurrentiel ou d'une opération d'activisme politique. Mais les plus fréquentes restent **les intrusions informatiques menées pour collecter des données à caractère personnel** par des extractions de bases de données clients ou autres **contrefaçons de fichiers.** Ce sont autant d'atteintes à la propriété intellectuelle de la part de compétiteurs indélicats à des fins d'exploitation pour économiser en investissement. Les escroqueries par le piratage des systèmes téléphoniques sont récurrentes car les entreprises oublient que l'autocommutateur téléphonique est un SI contenant des DCP et des messageries vocales à protéger[2]. Les fraudes internes sous-tendues par la vengeance ou les actions prud'homales, pour pénétrer les messageries des Directeurs de Ressources Humaines ou de supérieurs hiérarchiques, sont légion. Sont également en augmentation, mais la loi est récente[3], les usurpations de données personnelles afin de troubler la tranquillité de l'entreprise ou de porter atteinte à sa considération. Une incrimination qu'il ne faut surtout pas confondre avec la diffamation.

(2) ANSSI guide du PABX www.ssi.gouv.fr

(3) LOI n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure

L'origine des menaces : internes ou externes, tant du sabotage que de l'espionnage

Ces attaques utilisent le plus souvent les techniques du *watering hole* ou trou d'eau[4] pour faire du déni de service, de la défiguration des pages d'accueil des sites Internet d'associations, d'instituts, ou d'administrations. Ces actes de malveillance émanent le plus souvent d'activistes, de services de renseignements étrangers ou encore de mouvements du type *Anonymous*. Ils visent moins l'organisation elle-même qu'un secteur d'activité en particulier et peuvent chercher à mettre en cause des liens supposés entre une organisation et l'Etat.[5]

Le personnel prend rarement conscience du niveau de risque pris, le plus souvent par méconnaissance ou par absence d'identification des vulnérabilités. Mais on constate très fréquemment une utilisation non encadrée des technologies à disposition au sein de l'entreprise. Les intrusions dans les boites mails, les enregistrements de frappes sur les claviers d'ordinateurs, les infections virales de clefs USB ou des téléphones personnels, sont des pratiques courantes qui ne laissent pas de trace d'infraction. Par méconnaissance ou par négligence, les risques pris de façon non maîtrisée, deviennent rapidement des menaces pour la préservation du savoir-faire propre à l'entreprise, de son capital matériel et informationnel. Les conséquences peuvent se révéler désastreuses et restent en dernier recours à la charge de l'employeur. Attention toutefois pour ce dernier de ne pas instrumentaliser les services de ses techniciens pour surveiller de manière excessive ses employés, au point d'outrepasser parfois ses droits.

(4) Rapport Symantec sur les menaces de sécurité Internet 2012 http://www.symantec.com/fr/fr/about/news/release/article.jsp?prid=20130416_01

(5) www.zone-h.org

Des moyens encore sous-dimensionnés pour faire face à cette menace

La réalité doit être regardée en face pour limiter les risques. L'employé d'un sous-traitant informatique intégré à l'entreprise, est moins bien surveillé que nécessaire. En cas de litige, ses droits d'accès ne sont pas toujours invalidés à temps et l'on assiste à des suppressions de données ou des manipulations dans les systèmes. Ce qui peut avoir de lourdes comséquences pour l'entreprise ou ses clients.

A titre d'illustration, la suppression à distance d'archives médicales numériques a valu 14 mois d'emprisonnement avec sursis à son auteur. Celui-ci avait expliqué son acte par le fait que son contrat n›avait pas été reconduit. Il faut malheureusement souvent attendre ce genre de cas pour déclencher une prise de conscience et amorcer la réflexion au sein de l'entreprise sur les mesures de prévention à prendre. Tous les domaines de l'organisation sont concernés mais on estime que 80 % des infractions commises le sont par les personnes qui disposent d'un moyen informatique. Il y a longtemps que les services d'enquêtes spécialisés appellent de leurs vœux l'aggravation de peines, pourtant déjà fortes, afin de tenter d›éradiquer cette fraude interne. La Directive Européenne[6] du 12 août 2013 sur les incriminations va obliger la France à prendre, entre autre, ce type de mesure d'ici sa transposition finale en 2015.

> La réalité doit être regardée en face pour limiter les risques.

Le travail des RSSI, des DSI, des Correspondants Informatique & Libertés (CIL), de la CNIL, les alertes et les messages délivrés par les autorités, les formations conduites par l'INHESJ, l'ANSSI et dans les entreprises contribuent à faire progresser la cybersécurité. Ces actions renforcées par une production doctrinale cohérente avec les politiques publiques en matière d'Intelligence économique devraient permettre de faire reculer l'ignorance en la matière. La naïveté n'est plus de mise, ou relève alors de la paresse ou du manque de temps, voire d'un déni de réalité.[7] D'ailleurs la taille de l'entreprise ne sera pas prise en compte dans le règlement européen qui consolidera les déclarations sur les *data Breaches*[8] (vulnérabilités du système) et les violations de DCP. Une formation doublée de chartes de sécurité, d'une information du Comité d'entreprise et des syndicats commence à former un ensemble utile.

(6) DIRECTIVE 2013/40/UE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

(7) interview Nicolas Arpagian (INHESJ) http://www.bfmtv.com/high-tech/securite-informatique-gouvernement-on-ne-peut-plus-evoquer-lignorance-601262.html

(8) Le 24 Juin 2013, la Commission européenne a adopté un nouveau règlement n ° 611/ 2013 (le «Règlement») sur les mesures applicables à la notification des violations de données à caractère personnel prévues par la directive 2002/58/CE (la «Directive sur la vie privée »). Ce règlement est entré en vigueur le 25 Août 2013.

Les moyens pour faire face à cette menace : des produits et de la formation

L'entreprise doit se résigner à investir non seulement dans l'installation de moyens techniques de sécurité mais aussi dans un dispositif de sensibilisation de son personnel aux risques et aux menaces auxquels il est exposé. Par ailleurs, le ciblage de profils de meilleur niveau concernant les responsables de la sécurité des Systèmes d'Informations, capables de veiller à la e-reputation de l'entreprise tout autant qu'à l'analyse des traces de connexion se révèle impératif dans un dispositif de prévention des risques.

Le métier de RSSI, par principe en interconnexion permanente avec les services juridiques, des ressources Humaines et de la communication, doit également faire l'objet d'une revalorisation en interne. L'enjeu est d'être entendu au sein des comités de direction et de convaincre la Direction générale de la nécessité de consacrer les moyens nécessaires et suffisants pour installer un dispositif de protection efficace pour l'entreprise. Cela devrait se traduire concrètement par un repositionnement auprès de la Direction générale et par une augmentation des budgets dédiés à la sécurité-sûreté.

L'entreprise doit se résigner à investir non seulement dans l'installation de moyens techniques de sécurité mais aussi dans un dispositif de sensibilisation de son personnel aux risques et aux menaces auxquels il est exposé.

Les entreprises réagissent de plus en plus judiciairement face à ces attaques

Des procédures et moyens de réparation sont déployés mais plutôt dans les grandes entreprises qui ont plus de moyens à y consacrer.
Il s'agit d'identifier les bons interlocuteurs du côté des services de la Police et de la Justice et travailler en bonne coopération avec eux. Cela vient compléter les *process* de prévention et de gestion des risques mis en place au sein de l'entreprise. **Les actions de sensibilisation assurées par les services de l'Etat ou par les conférenciers en sécurité économique, labellisés par l'INHESJ et la D2IE, interviennent auprès des entreprises** par le reporting des RSSI ou des DSI.[9] Un constat doit être tiré au regard des chiffres relatifs aux plaintes en nette augmentation depuis 5 ans. Il nous rappelle qu'en dehors du RSSI, c'est tout le personnel de l'entreprise qui est concerné et qui doit s'impliquer, chacun à son niveau, dans la prévention des risques et la gestion des menaces.

Les actions de sensibilisation assurées par les services de l'Etat ou par les conférenciers en sécurité économique, labellisés par l'INHESJ et la D2IE, interviennent auprès des entreprises

L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) demeure un bon relais pour gérer les conséquences des attaques affectant les administrations et les opérateurs d'Importance Vitale (OIV). **Quant aux services des sociétés (privées) de sécurité, il s'agit de s'assurer de la qualité de leur prestation et d'un niveau de déontologie qui doit rester cohérent et complémentaire avec les actions de l'Etat.** Un travail d'identification et de vérification des professionnels en question est donc nécessaire.

Le Livre blanc sur la Défense et la Sécurité nationale de 2013 et la future Loi sur la programmation militaire[10] évoquent la question par les capacités défensives et offensives de l'ANSSI et du Centre d'analyse de lutte informatique défensive (CALID)[11] regroupés en un même endroit pour mieux se coordonner.

Les moyens consacrés à la préservation des données de l'entreprise, de son capital informationnel, ne seront jamais suffisants au regard de la rapidité à laquelle évolue et s'amplifie la cybermenace. Certains sont techniques et coûteux, d'autres, tout aussi essentiels, sont humains et demandent surtout un peu d'attention au quotidien. Il s'agit avant tout d'instaurer les bons réflexes à mettre en place dans l'utilisation des technologies de l'information. Ce qui relève d'abord de règles de bon sens et de partage de bonnes pratiques entre les entreprises. **Il s'agit enfin d'un bon niveau de coopération public-privé qui garantisse la circulation de l'information et l'identification d'interlocuteurs fiables en cas de crise majeure.** ■

(9) Le Cercle de la sécurité, CESIN, Les Assises de la Sécurité, Forum International de la cybersécurité.

(10) http://www.defense.gouv.fr/sante/actualites/projet-de-loi-de-programmation-militaire

(11) http://www.defense.gouv.fr/actualites/dossiers/sept-2011-cyberdefense-enjeu-du-21e-siecle/france/voir-les-articles/le-calid-l-expert-technique-en-securite-informatique-du-ministere

Par **Myriam QUÉMÉNER**
Magistrat

Quelles sont **les contraintes** et **les réponses** des **magistrats** pour traiter les affaires **cybercriminelles** ?

Les infractions servant de base légale à la répression de la cybercriminalité ont toutes pour dénominateur commun d'utiliser les réseaux numériques tantôt en tant qu'objets de l'infraction, tantôt en tant que supports de l'infraction [1] et enfin en tant que moyens de l'infraction. Un nombre croissant de malfaiteurs exploitent la rapidité et la fonctionnalité des technologies numériques, ainsi que l'anonymat qu'elles offrent, pour commettre des infractions comme le piratage des données et des systèmes informatiques, le vol d'identité, la diffusion d'images de pédopornographie, ou les escroqueries sur Internet.

Cette délinquance très transversale a donc bien évidemment fait son entrée dans les prétoires et interpelle de plus en plus souvent juges et procureurs. Il s'agit pour la justice[2] d'un contentieux encore nouveau qu'elle doit aborder avec détermination tant les enjeux économiques, financiers et stratégiques sont forts. Les magistrats doivent aujourd'hui comprendre qu'il s'agit désormais d'un contentieux à part entière, où le cybercrime n'est pas virtuel, et prendre la mesure d'un phénomène où les frontières volent en éclat.

Le traitement judiciaire de la cybercriminalité se heurte à de nombreuses contraintes tant juridiques qu'institutionnelles qu'il convient tout d'abord de présenter avant d'envisager les solutions et perspectives mises en place pour améliorer le traitement des « cyberprocédures ».

(1) F.Chopin, Maître de conférences HDR à l'Université d'Aix-Marseille II répertoire de droit pénal et de procédure pénale, Dalloz, mai 2009 (dernière mise à jour janvier 2013)

(2) M.Quéméner,Y. Charpenel, «Cybercriminalité, droit pénal appliqué, Economica, 2010

➔ RETOUR AU SOMMAIRE

Les contraintes juridiques

Un éparpillement des textes

Aujourd'hui, il apparait que les normes relatives à des infractions pouvant relever de la cybercriminalité sont dispersées dans divers codes, allant du code pénal au code de la propriété intellectuelle. Au rythme d'un texte par an en moyenne sans cohérence d'ensemble, le droit du numérique est aujourd'hui un véritable «millefeuille législatif et règlementaire» [3]. Depuis la loi n°78-17 du 6 janvier 1978 dite « Informatique et Libertés et la loi Godfrain [4], plusieurs lois sont intervenues dans le domaine de la cybercriminalité. Au niveau international, les États ont pris conscience de la nécessité d'une approche transfrontalière de la cybercriminalité, notamment en raison de la dimension internationale de cette forme de délinquance, avec par exemple la Convention de Budapest de 2001.

(3) Bertrand Boyer, Cyberstratégie, l'art de la guerre numérique, Paris, Nuvis, 2012, p. 104.

(4) Loi n° 88-19, 5 janv. 1988, relative à la fraude informatique, JO 6 janv. 1988, p. 231.

Les contraintes spacio-temporelles

La cybercriminalité est par essence planétaire puisque les infractions peuvent être commises simultanément dans plusieurs pays. Son traitement nécessite donc d'adopter une approche internationale. La lutte contre la cybercriminalité se heurte aussi aux difficultés inhérentes à l'entraide pénale internationale. L'impossibilité d'appliquer les normes françaises aux opérateurs étrangers peut rendre inefficace l'action judiciaire.

Les infractions commises sur Internet génèrent des difficultés, d'une part, dans la mise en œuvre des règles de compétence territoriales des juridictions pénales, d'autre part, dans l'application des délais de prescription de l'action publique.

Une infraction commise à l'autre bout du monde, peut avoir des effets sur le territoire français. De nombreuses procédures nécessitent ainsi la poursuite d'investigations à l'étranger. Mais elles connaîtront des résultats inégaux suivant le degré de coopération établi avec les pays concernés.

Les contraintes dans le recueil des preuves numériques

Vecteur et cible d'une criminalité polymorphe, Internet ignore les frontières et pose des défis considérables à la procédure pénale [6]. Bien qu'en matière de preuve pénale tous les moyens de preuve soient admis [7] (c. pr. pén., art. 427), lesdites preuves peuvent s'avérer difficiles à rapporter dans l'environnement numérique. Car elles sont volatiles et facilement modifiables par les « cyberdélinquants ».Cette difficulté s'aggrave si les données se trouvent dans un serveur localisé à l'étranger. Aussi, les règles gouvernant la collecte de la preuve en matière pénale ont dû être adaptées afin de permettre aux autorités de police et judiciaire d'appréhender des infractions à caractère dématérialisé et transnational [8]. **L'absence d'harmonisation des modes de recueil de la preuve pénale rend les procédures pénales inefficaces en matière de cybercriminalité.**

Vecteur et cible d'une criminalité polymorphe, Internet ignore les frontières et pose des défis considérables à la procédure pénale [6]

(5) Geneviève Giudicelli-Delage « Les transformations de l'administration de la preuve pénale », Archives de politique criminelle 1/2004 (n° 26), p. 139-188. URL : www.cairn.info/revue-archives-de-politique-criminelle-2004-1-page-139.htm.

(6) Article 427 du Code pénal

(7) Christiane Féral Schuhl, « la collecte de la preuve en matière pénale» , Revue Actualité pénale Dalloz , n° 3-2009.

➔ RETOUR AU SOMMAIRE

Les contraintes organisationnelles

Face à la criminalité numérique, les services de police et de gendarmerie se sont mis progressivement en ordre de bataille avec la création de services spécialisés. L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication l'Oclctic[9] en est un exemple. Au niveau de la Justice, si l'on note depuis une trentaine d'année une spécialisation croissante des juridictions, que ce soit en matière économique et financière ou des crimes contre l'humanité, tel n'est pas encore le cas dans le domaine de la cybercriminalité.

L'institution judiciaire ne mesure encore que partiellement l'ampleur qu'a pris le numérique dans notre société et la gravité de ses incidences à la fois sociétales, économiques et procédurales. **Tous les pays européens, à l'exception de la France, sont dotés de services dédiés à la lutte contre la cybercriminalité au niveau des administrations centrales.**

Tous les pays européens, à l'exception de la France, sont dotés de services dédiés à la lutte contre la cybercriminalité au niveau des administrations centrales.

Bien que les conséquences économiques soient très importantes, il n'existe pas encore de politique pénale dans ce contentieux ni de formation initiale suffisante. S'il existe une session de formation continue[10] dispensée par l'Ecole nationale de la Magistrature (ENM), celle-ci n'est toujours pas obligatoire.

Au niveau des juridictions interrégionales spécialisées (JIRS) qui auraient vocation à traiter les affaires de ce type, souvent à dimension financière ou avec des ramifications internationales, on constate qu'elles ne sont pas systématiquement saisies et pas encore assez sensibilisées sur les problématiques liées à la cybercriminalité.

L'absence d'identification d'interlocuteurs empêche le ministère de la Justice de participer aux travaux officiels tant au niveau national qu'international. Le préjudice est d'autant plus important dans un domaine qui se joue des frontières.

La France qui a par ailleurs un arsenal législatif tout à fait pertinent en matière de lutte contre la cybercriminalité devrait renforcer sa place sur la scène internationale.

La France qui a par ailleurs un arsenal législatif tout à fait pertinent en matière de lutte contre la cybercriminalité devrait renforcer sa place sur la scène internationale. On constate enfin de nombreuses initiatives très pertinentes malgré un éparpillement des actions et des structures. Certaines d'entre elles pourraient être mutualisées à l'heure où les restrictions budgétaires sont nécessaires et indispensables. Un effort de lisibilité doit être fait pour y remédier.

On assiste à des évolutions progressives afin de mieux répondre à cette délinquance numérique.

(8) Crée par décret interministériel du 15 mai 2000

(9) Dirigée actuellement par M. Quéméner

Les réponses de la justice face à la cybercriminalité

Des moyens d'investigation dédiés au numérique

L'infiltration consiste, aux termes de l'article 706-81 du Code de procédure pénale issu de la loi n° 2007 -297 du 9 mars 2004 portant sur l'adaptation de la justice aux évolutions de la criminalité, *« à surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes, comme un de leurs coauteurs, complices ou receleurs »*. Elle est un outil privilégié pour tout enquêteur qui découvre des agissements susceptibles de constituer une infraction. Elle permet par exemple d'intervenir, de façon dissimulée, sur un forum de discussion ou sur des sites. Il s'agit d'une technique d'enquête d'exception qui ne doit être utilisée que par des enquêteurs spécialement habilités, centraux ou territoriaux et seulement dans le cadre des investigations concernant des infractions prévues par l'article 706-73 du Code de procédure pénale.

L'infiltration est également possible, lorsque la loi le prévoit, pour les crimes et délits commis en bande organisée, autres que ceux relevant de l'article 706-73 du Code de procédure pénale. Elle est également pour les délits d'association de malfaiteurs prévus par le deuxième alinéa de l'article 450-1 du code pénal autres que ceux relevant du 15° de l'article 706-73.

La loi autorise l'agent infiltré à recourir à une identité d'emprunt et, si nécessaire, acquérir, détenir, transporter, livrer ou délivrer des substances, biens, produits, documents ou informations tirés de la commission des infractions ou servant à leur commission, sans être responsable pénalement de ces actes.

La loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance (article 35-III) a modifié le Code de procédure pénale pour permettre aux officiers de police judiciaire spécialement habilités de recourir à des infiltrations afin de faciliter la constatation de certaines infractions et *« lorsque celles-ci sont commises par un moyen de communication électronique , d'en rassembler la preuve et d'en rechercher les auteurs. »*.

L'article 706-35-1 du code de procédure pénale autorise le recours à cette technique pour constater les infractions les plus graves [11] comme notamment la diffusion de matériels pédopornographiques, les infractions en matière de proxénétisme, la prostitution de mineurs et la traite des êtres humains sur Internet.

L'article 706-47-3 du Code de procédure pénale introduit l'enquête dite de *« cyberpatrouille »*. Il autorise le recours à la technique d'infiltration *« dans le but de constater les infractions mentionnées aux articles 227-18 à 227-24 du Code pénal et, lorsque celles-ci sont commises par un moyen de communication électronique, d'en rassembler les preuves et d'en rechercher les auteurs »*.

Cette disposition permet ainsi à un officier ou un agent de police judiciaire spécialement habilité, et agissant dans le cadre d'une enquête préliminaire ou de flagrance ou à la demande d'un juge d'instruction sur commission rogatoire, de participer sous un pseudonyme aux échanges électroniques. Par ce moyen, elle permet aussi d'être en contact avec les personnes susceptibles d'être les auteurs d'infractions sexuelles, d'extraire, de transmettre en réponse à une demande expresse, d'acquérir ou de conserver des contenus illicites dans des conditions fixées par décret.

(10) articles 225-4-1 à 225-4-9, 225-5 à 225-12 et 225-12-1 à 225-12-4

(11) Voir Agathe Lepage, « Les dispositions concernant la communication dans la loi du 5 mars 2007 relative à la prévention de la délinquance », Communications-Commerce électronique, Revue mensuelle LexisNexis Jurisclasseur, juin 2007.

Ils peuvent ainsi collecter des preuves d'infractions en matière de traite des êtres humains, de proxénétisme et de recours à la prostitution des mineurs commises par un moyen de communication électronique.

Il convient d'observer que ces actes ne peuvent constituer une « incitation » à commettre ces infractions à peine de nullité. L'agent ne doit pas user de provocation à la commission de l'infraction. *« C'est la provocation à la preuve de l'infraction qui est admise et organisée par ces nouvelles dispositions, et non pas une provocation à la commission même de l'infraction »* [12].

Les articles D. 47-8, D. 47-9 et D.47-11 du Code de procédure pénale encadrent strictement les modalités d'intervention de ces officiers de police judiciaire spécialisés sur le réseau Internet. Cette mesure d'investigation nouvelle doit être préalablement autorisée par l'autorité judiciaire par écrit et spécialement motivée. Elle doit ainsi mentionner les infractions recherchées, l'identité de l'officier de police judiciaire responsable de l'opération et sa durée, de quatre mois maximum renouvelable.

Dès lors, ces officiers ou agents spécialement habilités peuvent participer sous un pseudonyme à des actions de jeux en ligne.

Les jeux d'argent et de hasard en ligne peuvent aussi donner lieu à ce moyen d'investigation depuis la loi n° 2010-476 du 12 mai 2010 ouvrant à la concurrence et à la régulation les secteurs des jeux d'argent et de hasard en ligne.

Les officiers de police judiciaire, spécialement désignés par le ministre de l'intérieur et les agents des douanes désignés par leur ministre de tutelle, peuvent désormais faire de l'infiltration pour constater les infractions commises à l'occasion de paris ou de jeux d'argent ou de hasard en ligne. Pour les agents des douanes, cette compétence est confiée à la fois au service nationale de douanes judiciaires et à la cellule « *Cyberdouane* » rattachée à la Direction nationale du renseignement et des enquêtes douanières (DNRED).

Dès lors, ces officiers ou agents spécialement habilités peuvent participer sous un pseudonyme à des actions de jeux en ligne. Cette technique d'investigation leur permet de récupérer et de conserver des données sur les personnes susceptibles d'être les auteurs d'infractions, sans en être pénalement responsables et sans que ces actions aient pour but de provoquer ces personnes à commettre ces infractions aux termes de l'article 59 de la loi du 12 mai 2010.

Captations de données à distance

La loi d'orientation de programmation et de performance sur la sécurité intérieure (Loppsi 2) a introduit la captation de données informatiques qui permet aux officiers de police judiciaire (OPJ) « *commis sur commission rogatoire de mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur* ».

Ce dispositif, qui consiste à placer un cheval de Troie à l'insu de la personne soupçonnée, sera utilisé avec des garanties procédurales strictes et notamment sous le contrôle d'un magistrat. Cette procédure ne concernera que les infractions les plus graves (terrorisme, pédophilie, meurtre, torture, trafic d'armes et de stupéfiants, enlèvement, séquestration, proxénétisme, extorsion, fausse monnaie, blanchiment et aide à l'entrée et séjour d'un étranger), commises en bande organisée.

Formation des magistrats et juridiction cyberspécialisée

Il est intéressant de rappeler que suite à de précédents travaux de politique pénale dans le ressort des cours d'appel de Paris et de Versailles, **des magistrats référents en cybercriminalité ont été mis en place dans la plupart des parquets de ces ressorts. Cette organisation doit être pérennisée. La plupart d'entre eux suivent une session de formation continue sur la cybercriminalité qui est proposée par l'Ecole Nationale de la Magistrature.**

Le rapport Bockel [13] a d'ailleurs préconisé la création d'un pôle juridictionnel spécialisé à compétence nationale pour réprimer les atteintes graves aux systèmes d'information.

Des magistrats référents en cybercriminalité ont été mis en place dans la plupart des parquets de ces ressorts.

Perspectives

Les réponses institutionnelles à la cybercriminalité sont en pleine évolution. En témoigne la mise en place d'un groupe de travail interministériel présidé par un haut magistrat dédié à cette délinquance numérique et à la protection d'Internet. Les conclusions du rapport devaient être remises fin novembre 2013 [14]. **Les préconisations du rapport devraient permettre d'adapter le droit matériel et processuel mais aussi d'apporter des réponses opérationnelles. L'objectif à terme étant d'améliorer le traitement judiciaire des affaires de cybercriminalité tout en renforçant la protection des cyber-victimes [15].**

(13) La cyberdéfense : un enjeu mondial , une priorité nationale Rapport d'information n° 681 (2011-2012) de M. Jean-Marie BOCKEL, fait au nom de la commission des affaires étrangères, de la défense et des forces armées, déposé le 18 juillet 2012, www.senat.fr

(14) http://www.pcinpact.com/news/82121-un-rapport-interministeriel-sur-cybercriminalite-prevu-pour-fin-novembre.htm

(15) Voir site: www.inavem.org , colloque 2013 sur les cybervictimes

Par **Etienne DROUARD**,
Chargé d'enseignement à l'INHESJ,
Avocat à la Cour, cabinet K&L Gates.

La nationalité d'un prestataire peut-elle faire la différence ?

Quand vient le moment du choix d'un prestataire, l'importance de sa nationalité semble encore résiduelle par rapport aux prix et à la fiabilité de la prestation. De nombreux paramètres peuvent expliquer ce relatif désintérêt pour la « préférence nationale ». Lorsqu'on ne peut pas « acheter local », il est essentiel de mesurer les enjeux contractuels, réglementaires et géopolitiques d'un partenariat avec un prestataire étranger.

L'affaire *Snowden* a montré à la face du monde que les géants du web, aussi multinationaux ou planétaires qu'ils soient, ont une nationalité. Qu'ils le veuillent ou non. Que leurs clients et usagers en aient ou non mesuré les conséquences.

La contribution des grands fournisseurs de services informatiques américains à l'action régalienne des Etats-Unis, a pu faire naître de grands espoirs à certains acteurs industriels et institutionnels européens. Surfer sur la peur de l'étranger, affirmer ses frontières, parler de « préférence européenne ». Ou comment transformer une crise médiatique et politique en opportunité industrielle.

Cap Gemini ou SAP n'ont-ils pas conçu en quelques semaines une initiative commerciale en faveur d'une « ligne Maginot » de l'hébergement européen ? Non. Leur offre conjointe était déjà sur le marché depuis de nombreux mois. Mais quel splendide espace publicitaire gratuit que l'engouement des médias à rechercher des marqueurs patriotiques face à une crise géopolitique transatlantique.

La vice-Présidente de la Commission européenne, Vivian Reding, n'a-t-elle pas voulu convoquer dans son bureau Barack Obama au lendemain des révélations du *Guardian* sur les activités de la NSA[1] dans le cadre du programme *Prism* ? Elle peut remercier l'apatride *Snowden* d'avoir donné un second souffle à la réforme européenne qu'elle porte depuis janvier 2012 en matière de protection des données personnelles et de la vie privée[2]. Voici qu'elle propose désormais la création d'une agence européenne de renseignement, prenant la NSA pour modèle.

Et « pendant ce temps-là... », les entreprises européennes rechignent-elles à nouer des accords commerciaux avec des prestataires extra-européens ? Pas sensiblement, voire pas du tout. Certes, des questions sont posées. Des consultants consultés. Des négociations s'approfondissent. Mais il ne semble pas qu'une vague de défiance anti-américaine ait renversé le cours des négociations contractuelles - quand il peut y en avoir - que nos entreprises conduisent avec leurs prestataires étasuniens.

La prise de conscience des enjeux que recèle un contrat international de prestations de services n'entraîne pas de paranoïa. Il y a lieu de s'en féliciter, si l'on veut améliorer la qualité des processus décisionnels dans ce domaine. Ces enjeux ont principalement trait à la géopolitique, à l'aléa réglementaire et à la négociation des contrats sur des volets non commerciaux. Aidons nos entreprises, quelle que soit leur taille, à les appréhender.

(1) National Security Agency - http://www.nsa.gov/.
(2) http://ec.europa.eu/justice/data-protection/index_fr.htm

Un « Yalta numérique » a eu lieu. Sans l'Europe.

En juin 2013, le président chinois Xi Jinping s'est entretenu officiellement avec le président américain Barack Obama des tensions grandissantes entre les deux superpuissances, suscitées par le cyber espionnage. Faisant suite à des accusations officielles formulées début 2013 par la Maison Blanche contre Pékin, cette entrevue s'est soldée par un accord de coopération sino-américain en matière de cybercrime et de cybersurveillance.

La stratégie de nos Etats et de nos entreprises ne peut donc, à moyen terme, reposer sur le repli ou l'affrontement. Elle impose un effort résolu de négociation et de partenariats entre Etats, au bénéfice de leurs entreprises.

Cet accord prévoit l'organisation de dialogues réguliers et institutionnels au plus haut niveau, destinés tant à identifier les auteurs d'attaques informatiques extérieures aux deux protagonistes, qu'à endiguer la cyber-guerre qu'ils se livrent en matière économique, militaire et géostratégique. Ce n'est qu'un point de départ, certes. Mais il est bi-partite et augure pour les années à venir d'un « Yalta numérique » auquel les européens n'ont pas pris part -ni les BRICS, pas plus que le reste du monde.

Dans ce contexte, les entreprises et les Etats européens devront trouver rapidement leur place. Certes, les logiciels « libres » sont performants et évolutifs. Certes, de nombreuses sociétés européennes et françaises proposent des services innovants, qui s'exportent et jouissent d'infrastructures de télécommunications performantes.

Mais il nous faut admettre que l'offre informatique dont nos PME ont les moyens, reste souvent dominée par des acteurs nord-américains, notamment en matière de systèmes d'exploitation, de cloud computing, de bureautique intégrée, de normes de paiement électronique, de commerce électronique hébergé, de publicité et de référencement, etc. La culture américaine de la propriété intellectuelle et des brevets logiciels favorise des solutions « propriétaires ». La nationalité de ces prestataires mondiaux détermine leur soumission à une définition régalienne et économique de la « sécurité nationale » qui ne connait pas de frontières.

La stratégie de nos Etats et de nos entreprises ne peut donc, à moyen terme, reposer sur le repli ou l'affrontement. Elle impose un effort résolu de négociation et de partenariats entre Etats, au bénéfice de leurs entreprises.

Connaître l'environnement réglementaire du prestataire

Les principaux critères de choix d'un prestataire qui peuvent emporter une décision d'achat, combinent le plus souvent deux facteurs déterminants : le prix de la prestation et la pérennité du prestataire. Ces deux facteurs sont pourtant les plus complexes à objectiver dans le secteur informatique, par exemple.

Le prix est peu aisément comparable et nécessite de savants et fastidieux calculs d'unités de compte, de frais de licence, d'intégration, de maintenance, d'évolution, de pénalités et bonus, de réversibilité, etc. La pérennité du prestataire, quant à elle, est extrêmement difficile à anticiper. Si celui-ci a le vent en poupe, il sera bientôt racheté par un actionnaire que ne garantira pas le maintien ou l'évolutivité d'une ligne de services. Si celui-ci peine à croître, il perdra ses hommes-clés sans qu'on sache s'ils partiront avec le cœur de la propriété intellectuelle ou du savoir-faire, incluant la compréhension des activités du client.

Lorsqu'une entreprise s'est acquittée de ses devoirs de comparaison tarifaire et de ses prédictions sur l'avenir d'un prestataire potentiel, il lui reste souvent peu de ressources à consacrer à la connaissance du cadre réglementaire qui entoure la nationalité du

prestataire. On pourra, avec obstination, tenter de soumettre le contrat à la loi française. Mais même si on y parvient, aucune des contraintes réglementaires qui s'imposent au prestataire dans son pays n'aura disparu.

Identifier ce qui ne se négocie pas entre entreprises

Voici quelques illustrations. Deux entreprises, l'une extra-européenne, l'autre européenne, quelle que soit la taille de cette dernière, ne négocient pas l'application du *Patriot Act* entre les murs de leurs cabinets d'avocats. Elles ne font pas, ni ne défont, les conventions fiscales conclues entre les Etats. Elles ne décident pas de la protection du secret des affaires et de la propriété intellectuelle que leurs garantissent leurs lois nationales respectives. Elles ne conviennent pas des normes internationales relatives aux paiements électroniques ou à la sécurité informatique. Elles ne peuvent déroger au droit processuel qui s'imposerait à l'une d'entre elles en cas de litige initié par un tiers. Elles ne déterminent pas les contraintes issues des réglementations comptable, bancaire, anti-corruption ou anti-blanchiment de leurs pays d'établissement respectifs. Elles ne peuvent s'accorder sur leurs obligations respectives en matière de cotation boursière, d'exportation de biens à double usage ou de cryptologie.

Même si elles choisissent la loi applicable à leur contrat, même si elles soumettent leurs différends éventuels à un arbitrage international, leurs activités et existences respectives sont dictées par des normes locales ou régionales qui déterminent un aléa réglementaire qui ne se contractualise pas, mais qui conditionne la sécurité du contrat qu'elles concluent.

La conscience du facteur réglementaire dans les relations contractuelles internationales reste à développer. Elle s'acquiert avec une formation, du temps et de la répétition.

Avant l'informatique en réseau, contracter à l'international était l'apanage des commissionnaires de transport, des armateurs, des avionneurs et des industriels ayant une forte activité exportatrice ou d'approvisionnement avec l'étranger. Il y a 20 ans, le droit du commerce international nourrissait des promotions de l'ordre de 300 nouveaux juristes par an en France.

Depuis l'informatique en réseau, l'achat d'un livre, d'un film, d'un vêtement, d'une solution de commerce électronique ou de cloud computing, concerne les particuliers, les TPE, les PME ou les grands groupes internationaux. En peu de temps et selon une répétition accrue, des dizaines de millions de consommateurs et des dizaines de milliers d'entreprises ont expérimenté en Europe des relations internationales avec peu ou pas de formation et en ayant à conclure ou négocier des contrats issus d'une autre culture juridique et réglementaire que celle qui les entoure. Le nombre de juristes internationalistes promus chaque année en France n'a que décuplé en 20 ans en France. Alors que les situations de droit international auxquelles ont à faire face les entreprises et les consommateurs sont devenues innombrables.

Deux grands rendez-vous réglementaires internationaux vont déterminer dans les trois années à venir les suites de ces expériences multiples du e-commerce international, en particulier transatlantique : la réforme européenne de la protection des données personnelles et les cycles de négociation « TTIP »[3] entre les Etats-unis et l'Union européenne.

Quelle stratégie européenne en matière de protection des données personnelles ?

Les deux textes en discussion depuis janvier 2012 au sein de l'Union européenne, un règlement[4] et une directive[5], touchent à des sujets essentiels, tant sur le plan économique, que régalien et démocratique. A l'heure où chacun s'accorde à constater que les données personnelles sont le carburant de l'économie numérique, il s'agit pour les institutions européennes de faire un choix stratégique à l'égard du reste du monde, notamment des Etats Unis -mais pas uniquement.

- Soit l'Europe veut renforcer le niveau de protection des données qui existait depuis 1995 et soumettre le reste du monde à ses règles internes, en prétendant imposer

(3) TTIP : Transatlantic Trade and Investment Partnership - http://ec.europa.eu/trade/policy/in-focus/ttip/#what_is_ttip

(4) Proposition de Règlement du parlement européen et du conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) - http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf

(5) Proposition de Directive du parlement européen et du conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données - http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_fr.pdf

sa réglementation à toute société -où qu'elle soit- qui traite des données personnelles concernant un ressortissant européen.

- Soit l'Europe veut exporter le niveau de protection des données qui existait depuis 1995 et négocier avec les Etats-Unis un socle commun de règles de protection des données, qui serait réciproquement valable de part et d'autre de l'Atlantique.

La première stratégie est celle qui est suivie aujourd'hui. La seconde hypothèse ne semble pas envisagée par les institutions communautaires. L'affaire *Prism* ne favorise pas l'émergence d'un dialogue en ce sens.

Pourtant, les cultures allemande, espagnole et britannique de la protection des données personnelles, ne sont pas plus proches l'une de l'autre, 18 ans après l'adoption de la Directive 95/46 du 24 octobre 1995[6], que ne l'est la législation californienne par rapport à la réglementation européenne actuelle.

Dans un environnement mondialisé, l'exportation des règles ne s'impose pas, elle se négocie.

L'acharnement européen contre les géants américains du web est un leurre. Il conduit à faire croire qu'en renforçant les contraintes qui pèseront d'abord sur les entreprises européennes, on se donnerait les moyens d'imposer au reste du monde des règles qu'on peine déjà à faire respecter sur le territoire européen. Dans un environnement mondialisé, l'exportation des règles ne s'impose pas, elle se négocie.

(6) Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML

Quelle stratégie européenne dans la conduite des négociations « TTIP » ?

Après avoir brandi son téléphone portable qui avait été mis sur écoute par la NSA, la Chancelière allemande a convenu que la tension provoquée par cette affaire ne devait pas mettre en péril les négociations commerciales Europe-Etats-Unis.

L'enjeu commercial de l'accord TTIP pour les deux régions est sans équivalent. Il porte sur le plus gros flux économique de la planète, représentant 30% du commerce mondial. Cet accord pourrait conduire à des tractations intersectorielles : harmonisation des normes automobiles contre reconnaissance mutuelle des législations pharmaceutiques, régulation financière renforcée contre subventions agricoles réduites (ou l'inverse). Dans le jeu des négociations, l'administration américaine dispose de liens bien plus étroits avec ses acteurs économiques, qui l'alimentent sur tous les sujets, que nos institutions communautaires avec nos fédérations professionnelles paneuropéennes.

Il ne faudra pas compter que sur la qualité technique de nos experts sectoriels pour déployer une stratégie d'influence efficace. L'imbrication des visions politiques et économiques européennes sera déterminante et peut bénéficier aux entreprises européennes, par la réduction de l'aléa réglementaire transatlantique. Elle sera une chance si les arbitrages finaux ne conduisent pas à défaire à l'égard de nos partenaires américains une réglementation européenne qui subsisterait pour le commerce intra-communautaire.

Les négociations contractuelles doivent dépasser les paramètres commerciaux

En droit international des affaires, une fois que la chose et le prix sont déterminés, il est impératif de désigner la loi applicable pour interpréter le contrat et régler les éventuels différends entre les parties. La particularité des prestations informatiques est qu'elles peuvent être régies par le droit d'un pays et être réalisées dans un ou plusieurs autres pays. **Il convient donc, surtout en matière de prestations dématérialisées, de mettre la géographie, la nationalité et la politique au premier plan des risques patrimoniaux.**

Le contrat peut être virtualisé, mais les données doivent être localisées

Il est de plus en plus aisé et courant de placer le règlement des litiges dans le cadre pragmatique d'un arbitrage ou d'une médiation internationale. C'est un gage d'expertise et de rapidité adapté aux situations impliquant plusieurs Etats. Quitte à être dans une situation dématérialisée, on peut ainsi virtualiser totalement le cadre du règlement d'un éventuel litige, qui sera tranché par des arbitres ou médiateurs compétents auxquels les parties se seront engagées à se remettre. Toutefois, ce n'est pas suffisant pour localiser une prestation et les enjeux réglementaires qui s'attachent à la nationalité du prestataire ou à la géographie d'une prestation.

On sait combien est difficile pour une société européenne contractant avec un prestataire multinational, de connaître la localisation des prestations qui lui sont fournies à distance : contrat-type non négociable, exclusions de responsabilité à outrance, pays ou Etat(s) d'hébergement inconnus, mécanismes de sauvegarde ou de redondance opaques ou modifiables instantanément, recours à la sous-traitance virtuelle ou distante.

Les entreprises européennes ne sont pas comme les autres

Qu'elle le veuille ou non, l'entreprise européenne, à la différence de toute autre dans le monde, supporte une obligation légale de savoir que ses données - lorsqu'elles sont à caractère personnel - sont susceptibles d'être traitées ou accessibles depuis un Etat non membre de l'Union européenne. Cette contrainte réglementaire qui pèse sur le donneur d'ordres européen, constitue un argument non négociable pour qu'il obtienne de son prestataire la plus grande transparence sur les lieux de ses prestations, ses sous-traitants et ses engagements de sécurité.

Songeons qu'en droit français, le fait de transférer -ou de rendre accessibles- des données personnelles hors de l'Union européenne sans en garantir une protection constante par le jeu de clauses contractuelles impératives ou d'engagements formels du cocontractant extra-européen, est passible de cinq ans d'emprisonnement et jusqu'à 1.500.000 euros d'amende.

La nationalité du prestataire compte

L'entreprise qui externalise une partie de ses actifs immatériels s'expose à la nationalité de son prestataire, puisque ce dernier ne peut échapper aux règles qui s'imposent dans son pays d'établissement, même si ses prestations sont réalisées depuis un autre pays que celui de sa nationalité.

Des solutions techniques -chiffrement chez le client, hébergement réparti sur plusieurs sites, etc.- peuvent pallier, dans une certaine mesure, le risque d'accès aux données de l'entreprise par une autorité étrangère à laquelle le prestataire étranger est soumis. Ces solutions supposent que l'entreprise européenne a connaissance du risque réglementaire qu'entraîne la nationalité de son prestataire. La connaissance de ce risque suppose un examen du droit local concerné, ce qui n'est pas à la portée de toutes les bourses.

Lorsqu'on n'a pas les moyens de contracter avec un prestataire extra-européen offrant un niveau satisfaisant de sécurité juridique et technique hors de l'Union européenne, il reste alors une dernière option de réduction du risque : choisir un ou plusieurs prestataires européens qui s'engagent à ne traiter les données qu'en Europe ■

Par **Thomas CASSUTO**
Magistrat, Docteur en droit

Quelle **place** pour la **coopération internationale** pour **lutter** contre la **cybercriminalité ?**

"Though change is inevitable, change for the better is a full-time job."
Adlai E. Stevenson - 1956

La cybercriminalité est une forme de criminalité qui par nature intègre les notions d'organisation et de mondialisation. Elle se développe en parasitant la révolution numérique permanente. La cybercriminalité recouvre des réalités multiples[1] qui ont ce point commun de se traduire par des actes dont les conséquences sont sans lien territorial avec le lieu de leur initialisation et qui peuvent porter atteinte aux intérêts vitaux d'un pays. Facteur aggravant, la réalité de la cybercriminalité est souvent minorée du fait de l'insuffisance des mesures de protection individuelles et des limites propres à l'action des autorités publiques.

(1) Pour la définition de la cybercriminalité, nous renvoyons aux articles 2 à 10 de la Convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001.

La cybercriminalité prospère à partir des principales failles des systèmes informatiques : leur mise en réseau et le facteur humain. Elle vampirise le net au point que les attaques les plus sévères résultent de réseaux de systèmes zombies[2]. **L'anonymat et l'absence de barrière physique favorisent le passage à l'acte dans des formes et selon des degrés de gravité variables.** Face à de telles menaces, et comme dans d'autres domaines, la militarisation des moyens de lutte contre la cybercriminalité constitue une des tendances répondant à la difficulté de lutter contre la criminalité transnationale.

L'anonymat et l'absence de barrière physique favorisent le passage à l'acte dans des formes et selon des degrés de gravité variables.

(2) Voir notamment le Rapport de la Commission au Conseil fondé sur l'article 12 de la décision-cadre du Conseil du 24 février 2005 relative aux attaques visant les systèmes d'information - COM(2008) 448.

Dans ses formes les plus graves, la lutte contre la cybercriminalité doit généralement intégrer un volet de coopération internationale. Cette composante doit être adaptée en permanence pour aborder les défis de la cybercriminalité.

Les moyens de la coopération internationale

La coopération judiciaire internationale s'appuie sur des outils juridiques et opérationnels.

Les outils juridiques

Au niveau international

La Convention du Conseil de l'Europe de novembre 2001 est le seul instrument international dédié à la lutte contre la cybercriminalité. Cet instrument constitue toutefois une référence dans ce domaine dans la mesure où elle a été signée et ratifiée par de nombreux États non européens, en particulier les USA et le Japon. Cette convention donne une définition élargie et consensuelle de la cybercriminalité. Elle prévoit également

des règles de procédures qui facilitent la coopération internationale. Elle prévoit par exemple, sous certaines conditions, le principe de la « perquisition en ligne ». Elle permet également d'accélérer la transmission des requêtes grâce au réseau des points de contact. Cette convention a inspiré de nombreuses législations nationales favorisant une meilleure coopération. Bien entendu, la question récurrente de sa modernisation se pose mais elle s'efface devant la nécessité de renforcer urgemment les ratifications laissant pour le moment subsister des havres pour les cybercriminels.

A défaut de pouvoir invoquer la Convention de Budapest, les autorités compétentes peuvent invoquer les instruments classiques de la coopération judiciaire qui permettent de traiter les preuves numériques au même titre et dans les mêmes conditions que les preuves classiques. Parmi ces instruments on peut citer la Convention des Nations Unies contre la criminalité organisée le 15 mai 2000 ou la Convention du Conseil de l'Europe de 1959 relative à l'entraide en matière pénale et ses protocoles additionnels.

Au niveau européen

Cette modernisation constante constitue le premier pilier de la coopération permettant d'offrir une base juridique interne conforme aux instruments internationaux. Le droit français offre des bases solides pour solliciter et accorder l'entraide avec d'autres pays.

La cybercriminalité constitue l'un des dix « eurocrimes » listés à l'article 83 du Traité sur le fonctionnement de l'Union européenne. Cette base juridique permet une harmonisation des infractions et des sanctions. Sur cette base, l'Union européenne a adopté la Directive 2011/92/UE du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie[3]. Cette directive harmonise une définition détaillée et extensive de la pédopornographie (art. 2) et les infractions liées à l'exploitation sexuelles des enfants (art. 4) et la pédopornographie (art. 5). Un tel instrument s'impose pour renforcer la coopération judiciaire afin de renforcer la garantie de double incrimination et un niveau minimum équivalent de sanctions.

La Commission européenne a également présenté en 2010 une proposition de directive relative aux attaques visant les systèmes d'information[4]. Cet instrument, toujours en cours de négociation, doit permettre de franchir un seuil dans l'harmonisation des définitions des infractions caractéristiques de la cybercriminalité et d'établir un seuil minimum commun de sanctions.

En matière de coopération judiciaire, la Convention d'entraide pénale entre les Etats membres du 29 mai 2000 est largement utilisée au sein de l'Union[5]. Cet instrument est susceptible d'être remplacé par la proposition de Directive relative à la décision d'enquête européenne[6] actuellement en cours de négociation. Ce projet, qui vise à mettre en œuvre le principe de la reconnaissance mutuelle prévu par l'article 82-1 du TFUE à toutes les demandes de recherche et de recueil de preuve, ne comporte pas de disposition particulière pour les preuves numériques. Il est néanmoins susceptible de s'appliquer sous couvert de dispositions dédiées au recueil de preuves en temps réel ou des interceptions de télécommunications[7].

Au niveau national

Le droit pénal spécial relatif à la lutte contre la cybercriminalité a été l'un des pionniers dans ce domaine. Il a été régulièrement adapté pour répondre à ces évolutions[8]. **Cette modernisation constante constitue le premier pilier de la coopération permettant d'offrir une base juridique interne conforme aux instruments internationaux. Le droit français offre des bases solides pour solliciter et accorder l'entraide avec d'autres pays.** L' efficacité de la coopération reposera en conséquence sur la compétence des acteurs et l'existence d'une base juridique satisfaisante dans l'autre Etat.

Les outils opérationnels

Au niveau international

La haute technicité qu'implique la lutte contre la cybercriminalité requiert l'agrégation de compétences nombreuses et variées et d'un niveau de compétence maximal dans des domaines tels que le *reverse engineering*, les réseaux informatiques, les télécommunications, etc. Cet impératif a conduit notamment Interpol ou encore d'Europol[9], à se doter de structures d'expertise interne calquées sur certains des dispositifs nationaux parmi les plus performants.

(3) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:FR:PDF. Elle remplace la décision-cadre 2004/68/JAI.

(4) http://eur-lex.europa.eu/LexUriServ/LexUriServ.

(5) A ce jour, seules l'Irlande, l'Italie et la Grève ne l'ont pas ratifiée.

(6) http://www.senat.fr/europe/textes_europeens/e5288.pdf . Cette proposition vise notamment à remplacer la convention de 2000 ainsi que la DC relative au mandat d'obtention de preuve.

(7) Plus généralement, v. Thomas Cassuto (dir.) « Une Europe, deux lois pénales », éd. Bruylant, 2012.

(8) V. Myriam Quemener, Yves Charpenel « Cybercriminalité - droit pénal appliqué », Economica 2010.

(9) L'OTAN a mis en place en 2012 une équipe de réaction rapide pour lutter contre les cyberattaques ; Interpol a mis en place un programme de lutte contre la cybercriminalité qui intègre des capacités d'expertise ; l'Union européenne a créé en janvier 2013 un Centre Européen contre le Cybercrime établi au sein d'EUROPOL (https://www.europol.europa.eu/ec3) .

(10) Telles que prévues notamment par la Convention UE du 29 mai 2000 et la Décision-cadre 2002/465/JAI.

Ces structures ont une triple mission : offrir en interne une expertise propre, assurer un rôle de coordination active peu dépendante des Etats et constituer un pôle de référence pour les Etats qui sont dépourvus des capacités internes pour analyser ou traiter une affaire. **Le lien naturel entre EUROPOL et EUROJUST permet en outre de renforcer les capacités de coopération au sein de l'UE et au-delà. La mise en œuvre d'équipes communes d'enquêtes[10] démontre que des outils procéduraux et opérationnels classiques peuvent parfaitement être adaptés pour lutter contre la cybercriminalité.**

Au niveau national

(11) Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication rattaché à la Direction centrale de la Police judiciaire.

Parallèlement à l'adaptation de sa législation, la France s'est dotée de capacités techniques et opérationnelles de pointe pour traiter la cybercriminalité. Ces capacités allient les services de protection et de réponse placés sous l'autorité du SGSDN (ANSII, CERTA) et l'intégration de compétences techniques au sein des services centraux de police judiciaire (police et gendarmerie). Ce dispositif qui gagnerait à être renforcé au niveau central permet l'échange d'information et la transmission de savoir-faire entre les niveaux. Dans le cadre de la coopération internationale, la pratique démontre que l'OCLCTIC[11] point de contact national 24/7, permet de traiter ou de relayer les demandes de coopération judiciaires actives et passives à bref délai.

Parallèlement à l'adaptation de sa législation, la France s'est dotée de capacités techniques et opérationnelles de pointe pour traiter la cybercriminalité.

Ce dispositif est par ailleurs intégré dans un schéma national de réponse aux atteintes informatiques en particulier lorsqu'elles ciblent des intérêts vitaux ou des structures publiques.

Perspectives

La lutte contre la cybercriminalité est un défi permanent. Le niveau des capacités de la France dans ce domaine n'est souvent qu'un maillon dans une longue chaîne. Les succès enregistrés ne doivent pas affecter notre niveau de vigilance et nos besoins d'adaptation face aux défis à venir. Pour ce faire, il est nécessaire d'actualiser notre doctrine pour l'adapter à l'évolution des menaces.

Quelle réponse apporter à la cybercriminalité transnationale ?

La cybercriminalité est un phénomène protéiforme évolutif caractérisé par une asymétrie variable incorporant une composante extraterritoriale récurrente. Cette asymétrie résulte du fait de la distorsion entre l'origine de la menace et ses conséquences : un individu isolé peut, à distance, provoquer des dégâts considérables. Cette asymétrie varie selon les auteurs, les cibles, les buts ponctuels ou récurrents recherchés. Pour illustrer cette problématique, la question se pose de qualifier l'origine de la menace (structure et localisation), la nature de la cible et les conséquences possibles. Face à ces différentes menaces plusieurs types de réponses sont possibles. L'analyse de ces paramètres peut permettre de déterminer la réponse appropriée. Qui peut être technique, administrative, judiciaire, voire militaire (v. tableau).

Cible / dommages Origine	Individuelle / conséquences limitées	Institutionnelle / conséquences limitées – risque pénalité	Intérêts fondamentaux / souveraineté
Individu	Réponse structurelle	judiciaire	judiciaire
Organisation criminelle	Réponse structurelle / judiciaire	Réponse judiciaire et gouvernementale	Gouvernementale (dont militaire ?)
Structure d'Etat ou organisation criminelle sponsorisée	judiciaire / gouvernementale	Judiciaire / gouvernementale	Militaire cybernétique (?) / conventionnelle / non conventionnelle ?

➔ RETOUR AU SOMMAIRE

Par ailleurs, la coopération internationale est un élément clef de la lutte contre les organisations terroristes qui ont parfaitement intégré les avantages que pouvaient leur apporter les technologies de l'information et de la coopération.

D'un côté de l'échelle, l'utilisation frauduleuse de la carte bancaire du « voisin » n'a de conséquences que patrimoniales et limitées par l'assurance qui accompagne le contrat de carte bancaire. A l'autre bout, une attaque d'une composante militaire d'un Etat vise des infrastructures critiques d'un autre Etat susceptible de porter atteinte à la sécurité physique des personnes et à la souveraineté de l'Etat. Dans ce dernier cas, la question de la légitime défense pourrait se poser et le cas échéant de la riposte la plus appropriée [12].

(12) V. Livre blanc « Défense et sécurité nationale 2013 » pp. 105 et s. http://www.gouvernement.fr/sites/default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf

Les succès de la coopération

Pour contrer la cybercriminalité, l'action judiciaire constitue une réponse légitime dans le cadre de l'Etat de droit. Face à la dimension internationale de la cybercriminalité, la coopération judiciaire est un impératif majeur. Elle doit permettre de traiter toutes les infractions, quels que soient leurs auteurs et en quelque lieu qu'ils se trouvent.

De nombreux exemples démontrent que les autorités nationales disposent des moyens et des compétences pour coopérer internationalement contre la cybercriminalité. Cette coopération constitue un formidable vecteur pour la mise en commun de ressources, le partage d'informations, d'expériences, et de savoir-faire. **Par ailleurs, la coopération internationale est un élément clef de la lutte contre les organisations terroristes qui ont parfaitement intégré les avantages que pouvaient leur apporter les technologies de l'information et de la coopération.**

La coopération internationale permet ainsi de lutter à tous les niveaux disponibles contre la cybercriminalité. En particulier, elle permet en amont d'atteindre les sites et les serveurs complices ou complaisants, de faire supprimer les contenus illicites, de limiter la porter des activités cybercriminels, et de réprimer les auteurs principaux. L'échange de preuves et d'informations au niveau international est à ce titre essentiel pour identifier, à partir des supports, les auteurs, mettre fin à leurs agissements et protéger les victimes.

Les sources de préoccupation

Si en règle générale on peut se féliciter des capacités d'action et des résultats, on observe que face à des organisations très structurées, des progrès restent à accomplir. Plusieurs causes l'expliquent. Le volume de la cybercriminalité ne permet pas encore de donner une réponse systématique. La variabilité des niveaux de compétence nationaux constitue parfois un frein à la prospérité des investigations notamment dans un pays qui ne dispose pas de compétences suffisantes ou qui ne dispose pas d'un cadre législatif approprié.

La protection des données

Les révélations récentes sur l'existence de programme de surveillance et d'interception des communications et de collecte des données personnelles affectent le niveau de confiance réciproque nécessaire à la coopération. Si le besoin de contrôle de l'espace « virtuel » répond à l'impératif de la protection de l'ordre public des menaces multiples (terrorisme, trafic de drogue, immigration clandestine, criminalité organisée, cybercriminalité, grande délinquance économique et financière) il se doit d'opérer en respectant les libertés individuelles. Sans oublier que la principale faille des systèmes informatiques se situe entre la chaise et le clavier.

Les révélations récentes sur l'existence de programme de surveillance et d'interception des communications et de collecte des données personnelles affectent le niveau de confiance réciproque nécessaire à la coopération.

C'est dans ce contexte que les instruments liés à la collecte, à l'échange international de données doivent satisfaire à des exigences accrues. Cette tendance s'illustre par exemple avec le paquet législatif présenté par la Commission européenne le 25 janvier 2012[13] composée d'une proposition de Directive relative au traitement des données à caractère personnel par les autorités compétentes en matière pénale[14], et d'une proposition de Règlement relatif au traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)[15]. Sous réserve du respect du principe de proportionnalité, et au bénéfice de garanties effectives et appropriées, toute information qui constituerait un élément de preuve doit pouvoir être accessible aux enquêteurs.

La coopération transatlantique est le témoin de cette tension. Les autorités américaines souhaitent pouvoir solliciter/requérir directement les entreprises qui détiennent des données personnelles. Le cadre judiciaire, c'est-à-dire le contrôle par l'autorité judiciaire, garante des libertés individuelles, demeure le cadre approprié pour collecter et exploiter les preuves recueillies y compris lorsqu'elles comportent des données personnelles.

(13) Pour un aperçu de la législation européenne applicable en matière de protection des données personnelles, voir http://ec.europa.eu/justice/data-protection/law/index_en.htm.
(14) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:FR:PDF
(15) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FR:PDF

Conclusion

La coopération judiciaire internationale est un élément essentiel de la lutte contre la cybercriminalité. Elle doit s'appuyer sur une expertise technique garantissant l'admissibilité et la libre circulation des preuves. Elle a sa place dans le cadre de dispositifs nationaux de lutte contre les formes les plus graves de criminalité. Elle peut s'appuyer sur des instruments juridiques et des capacités opérationnelles adaptés, quoique parfois sous-dimensionnés et qu'il conviendrait de renforcer.

Toutefois, pour être efficace, ce type de réponse doit être intégré dans une démarche plus globale de protection des systèmes informatiques passant par l'information du public, la sécurisation des dispositifs vitaux, les capacités d'anticipation et de réaction, et qui préviennent l'existence d'espaces ou de technologies hors de portée des autorités.

Entretien conduit par **Nicolas ARPAGIAN**,
le 14 octobre 2013

Entretien avec Pascal BUFFARD

Président du CIGREF

*Le CIGREF - Réseau de Grandes Entreprises - est une association créée en 1970, regroupant 138 grandes entreprises et organismes français. Sa mission est de **promouvoir la culture numérique comme source d'innovation et de performance**. Le CIGREF a crée avec l'INHESJ un Cycle de formation à la « Sécurité des usages numériques », dirigé par Nicolas Arpagian.*

La sécurité numérique est-elle désormais au menu des comités exécutifs des grandes entreprises françaises ?

La sécurité de l'information a toujours été une composante importante de la stratégie des entreprises, ne serait-ce que pour la protection des données confidentielles qu'elles détiennent. Mais si la sécurité était facilitée auparavant par une certaine autarcie du système d'information et que sa gestion en était donc confiée aux experts du domaine, il n'en est plus de même aujourd'hui. L'ouverture du monde de l'entreprise amène nécessairement un grand nombre de nouveaux risques numériques, et l'actualité récente montre en effet que ces risques sont avérés.

La sécurité n'est donc plus limitée à un débat d'expert mais bien portée au plus haut niveau stratégique, au niveau des comités exécutifs des entreprises, car elle a un impact fort sur leur pérennité. C'est ce message qui est porté par le CIGREF aux Assises de la Sécurité 2013, représenté par son vice-président Georges Epinette.

> La sécurité n'est donc plus limitée à un débat d'expert mais bien portée au plus haut niveau stratégique

Par ailleurs, si la sécurité est une thématique majeure au niveau stratégique, il ne faut néanmoins pas oublier que chaque salarié de l'entreprise en est un acteur déterminant ! Nous sommes donc en train d'élaborer un *Serious Game* en partenariat avec le Comité Richelieu pour favoriser la sensibilisation de tous à ces problématiques. Un premier scénario a d'ores et déjà été construit par la réflexion conjointe d'un groupe de travail CIGREF et la promotion 2012-2013 du cycle Sécurité Numérique CIGREF- INHESJ, sous le pilotage de Jean-Marc De Felice, Directeur des Ressources Techniques de Radio France.

Comment peut-on concevoir une sécurité des systèmes d'information dès lors que la tendance est à l'externalisation de ces équipements, qu'il s'agisse du recours au Cloud Computing ou à des sociétés de service tierces ?

Externalisation et sécurité ne sont pas des termes antinomiques dans le contexte de l'entreprise. Il ne faut pas oublier que la constitution d'une politique de sécurité des systèmes d'information passe par une analyse fine des risques. Dans ce cadre, toutes les données et les traitements qui les concernent ne nécessitent pas le même niveau de préoccupation, et doivent donc avoir une considération sécuritaire adaptée.

Cette problématique est d'ailleurs traitée par un guide rédigé conjointement par le CIGREF, l'IFACI et l'AFAI sur la protection des données dans le Cloud. Ce guide, à destination des dirigeants d'entreprises, a pour but d'aiguiller sur les réflexions à mener autour de la caractérisation des données selon leur degré de confidentialité et de leur externalisation possible on non dans les différents types de Cloud (interne/externe, public/privé). Bien entendu, tout ceci doit s'accompagner d'un socle technique et d'un cadre juridique solides.

Après les révélations sur le programme étatsunien PRISM, estimez-vous que les grandes entreprises considèrent désormais le critère de la nationalité pour se déterminer dans le choix d'un prestataire informatique ?

La révélation de PRISM est effectivement le dernier évènement en date, mais les questions liées au Patriot Act ou à ses équivalents dans d'autres pays font partie des préoccupations des entreprises depuis bientôt deux ans. Dans ce contexte, les entreprises considèrent effectivement le critère de la nationalité comme important dans le choix de prestataires qui seront amenés à jouer un rôle sur les parties sensibles du système d'information.

> Dans le contexte de la sécurité, l'Etat a un devoir de sensibilisation, qui est partagé par les entreprises. C'est pourquoi le CIGREF et l'INHESJ ont lancé ensemble le cycle de formation à la sécurité numérique

Qu'attendez-vous des services de l'Etat en matière de sécurité numérique ?

La sécurité numérique est une problématique qui dépasse de loin les frontières de l'entreprise, elle est globale ! Entreprises privées ou publiques et Etat se doivent donc de travailler main dans la main pour aborder ce sujet.

Dans le contexte de la sécurité, l'Etat a un devoir de sensibilisation, qui est partagé par les entreprises. C'est pourquoi le CIGREF et l'INHESJ ont lancé ensemble le cycle de formation à la sécurité numérique, dont l'objectif est de faire connaître aux acteurs décideurs de la sécurité en entreprise les tendances actuelles dans ce domaine, ainsi que l'ensemble des parties prenantes publiques et leur rôle.

Comment les entreprises évaluent-elles le risque numérique ? Quels sont les critères qui sont pris en compte?

Puisque le numérique a un caractère transversal dans l'entreprise, les risques liés ne sont pas circonscrits au seul périmètre des systèmes d'information. Le CIGREF a publié une étude sur ce sujet en 2011, qui avait pour objectif d'en établir une cartographie. 8 familles de risques ont donc été identifiées : ressources humaines, dématérialisation des rapports humains, stratégie, contrôle des systèmes d'information, éthique et juridique, patrimoine numérique, marketing et les risques périphériques.

Certains risques sont localisés, comme les risques marketing qui sont concentrés sur les relations avec les clients, et tous n'apparaissent pas au même moment. Alors que certains seront d'actualité tout au long de la vie de l'entreprise, comme ceux relatifs à la cybercriminalité, d'autres n'apparaissent qu'au moment du passage vers le numérique, pour s'estomper ensuite. C'est le cas du risque lié au manque d'adhésion des employés, ou celui lié à la concurrence entre supports de vente. Ces distinctions sont importantes lorsqu'il s'agit de chercher à faire de la prévention car les politiques de gestion des risques à court, moyen et long terme dépendent du moment où les risques sont susceptibles d'apparaitre.

Les critères à prendre en compte dans l'évaluation de ces risques sont donc la gravité de l'impact, l'occurrence (fréquence et instant), et le périmètre touché.

Direction des systèmes d'information, direction des risques, direction de la sécurité, direction générale… Selon votre expérience, quelle est la tutelle la plus pertinente pour que l'entreprise se dote de ressources efficaces en termes de sécurité numérique ?

La sécurité numérique en entreprise doit être portée par l'ensemble des collaborateurs. Tous ont un rôle important à jouer dans la protection de leur entreprise. **C'est pourquoi il est nécessaire que la communication sur ce sujet soit portée par les plus hautes instances dirigeantes au sein de l'entreprise,** pour que les bonnes pratiques de sécurité soient intégrées dans la culture et les valeurs de l'entreprise.

C'est la raison pour laquelle le CIGREF a souhaité créer une formation adaptée à ces nouveaux enjeux, en proposant un cycle de spécialisation à la « sûreté numérique ». Nous en sommes à la 4ème session et les auditeurs viennent de services très divers au sein des "Grandes Entreprises".

Le rattachement hiérarchique exact importe assez peu finalement, tant qu'une transversalité effective est appliquée entre les directions des systèmes d'information, des risques et de la sécurité pour la mise en œuvre des politiques de sécurité. Le point majeur restant que la direction générale doit apporter un sponsorship fort sur la démarche.

Le caractère potentiellement international d'une attaque informatique, au moins en ce qui concerne les moyens utilisés, serait-il de nature à vous à dissuader les entreprises de porter plainte si elles en étaient victimes victime ?

Sur le caractère international des attaques, nous ne pouvons pas nous défendre si nous ne collaborons pas en mettant en commun toutes les bonnes volontés. Il est donc important que les entreprises signalent les attaques subies par le dépôt de plainte, afin que l'analyse des faits puisse ne serait-ce que contribuer à la lutte contre la cybercriminalité et le cyberterrorisme. Il en va de la responsabilité civique de chacun.

Pensez-vous que les entreprises/institutions victimes de cyberattaques ne perdent plus de crédit lorsque celles-ci sont révélées, au motif que de telles annonces sont devenues quasi quotidiennes dans le monde ? Etes-vous favorable à une obligation de déclaration aux pouvoirs publics par l'entité ciblée en cas de cyberattaque constatée ?

Les mentalités changent en effet sur le sujet. C'est malheureux, mais la multiplication des attaques en est la cause. Si la compromission des systèmes de Sony en 2012 avait engagé des grandes manifestations de baisse de confiance des utilisateurs, on constate aujourd'hui que malgré les attaques à répétition sur les réseaux sociaux (Linked In, Twitter), ces baisses de confiance sont fortement limitées. L'atteinte à l'image de l'entreprise est toujours présente, mais est effectivement moindre aujourd'hui.

Sans parler d'obligation de déclaration, le rapprochement avec les organismes de sécurité publics est un atout qui doit être considéré. D'ailleurs, le CIGREF soutient l'Académie d'Intelligence Economique dans l'organisation de la journée nationale de l'IE dont la prochaine occurrence se tiendra le mercredi 4 décembre 2013 et aura pour thème l'impact du numérique sur l'influence des nations et des firmes, et sur notre rapport aux risques. ■

Pour aller plus loin

Travaux des auditeurs

La sécurité des smartphones

Les auditeurs de la 16ème session Nationale Spécialisée ont étudié, dans le cadre de leurs travaux d'études, sur l'environnement hautement concurrentiel de la téléphonie mobile. Premier moyen de connexion à Internet, l'utilisation du Smartphone s'est généralisée à des fins privées mais aussi professionnelles. Les enjeux de sécurité deviennent dès lors un enjeu majeur sur lequel il convient de se pencher.

Sur la base d'un travail de veille et d'analyse, 5 auditeurs, proposent d'analyser le positionnement des principaux Smartphones du marché en termes de sécurité.

➔ *Synthèse du GVA à télécharger*

➔ *Rapport du GVA à télécharger*

A signaler autour du sujet

Bibliographie

- *Au coeur de la cyberdéfense*, DSI N°32 Hors-série
- *Le Monde* du 31 Octobre 2013 : http://www.lemonde
- *Entreprises et culture numérique*, rapport du CIGREF, 2013.
- ARPAGIAN Nicolas, *La Cyberguerre – La Guerre numérique a commencé*, Vuibert, 2009.
- ARPAGIAN Nicolas, *La Cybersécurité*, Presses Universitaires de France (PUF), Collection Que Sais-Je ?, 2010.
- BOCKEL Jean-Marie, *Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées du Sénat sur la cyberdéfense*, n°681, Sénat, juillet 2012.
- BOYER Bertrand, *Cyberstratégie, l'art de la guerre numérique*, Nuvis, 2012.
- Collectif, *Livre Blanc sur la Défense et la sécurité nationale*, La Documentation Française, 2013.
- FREYSSINET Eric, *La Cybercriminalité en mouvement*, Hermès Lavoisier, 2012.
- HARREL Yannick, *La cyberstratégie russe*, Nuvis, 2013.
- TKACHEVA Olesya , Schwartz Lowell H. , Libicki Martin C. et Taylor Julie E. *Internet freedom and political space*, Rand Corporation, 2013.
- PINTE Jean-Paul & QUÉMENER Myriam, *Cybersécurité des acteurs Economiques*, Hermès Lavoisier, 2012.

Veille Cybersécurité

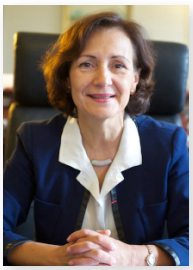
Par Fabian RODES, Auditeur INHESJ de la 16ième session nationale spécialisée.

D'un rapide passage en revue de sites institutionnels et privés, de journalistes ou bloggeurs, d'articles et de documents thématiques, se dégagent 3 notions phares qui structurent le champ de la Sécurité dans le cyberespace : la cybersécurité, la cybercriminalité, et la cyberdéfense.

Ce document propose une sélection non-exhaustive des principaux sites d'information Internet qui se consacrent au sujet de la Sécurité au sein du cyberespace. Leur classement ci-après mentionne la dominante de l'une des trois notions évoquées, dont voici une proposition de définition reprenant la terminologie communément admise sur les différents sites et rapports institutionnels (...)

➔ *Lire la suite en ligne*

Entretien conduit par **Diane DE LAUBADÈRE**
Chargée de mission, Département sécurité économique
le 22 octobre 2013



Entretien avec Claude REVEL

Cinq mois après sa nomination, Claude Revel, la déléguée interministérielle à l'Intelligence économique, revient sur le nouveau dispositif de politique publique voulue par le gouvernement. Chargée par le Premier ministre de mettre en place une stratégie innovante en matière d'intelligence économique, la déléguée à la D2IE présente ici sa vision et les leviers essentiels de son action que sont la formation, l'anticipation, la sécurité et l'ingénierie d'influence.

Quelles avancées et freins majeurs identifiez-vous dans l'acculturation des services de l'Etat comme des entreprises à l'intelligence économique ?

Après trois mois de présence, je peux vous annoncer une bonne nouvelle : il y a une forte appétence pour l'intelligence économique de la part de très nombreux interlocuteurs au sein de l'Etat et des entreprises. Je suis approchée par de nombreuses personnalités, venant de ministères comme du secteur privé, qui me présentent des dossiers, des propositions, et aussi des cas problématiques pour lesquels nous essayons de proposer des solutions. Cela nous met d'ailleurs une certaine pression, car l'attente est grande vis-à-vis de notre Délégation. J'ai l'impression que la demande territoriale est forte, sans doute parce que, en région particulièrement, les acteurs vivent sur le terrain de la compétition quotidienne. En face de cela, il y a encore dans l'administration, et c'est la mauvaise nouvelle, quelques réticents impénitents dont le caractère minoritaire est parfois inversement proportionnel à la résistance qu'ils peuvent mettre en œuvre : résistance au changement d'état d'esprit, à la vision transversale, au décloisonnement des approches, certitudes inébranlables que ce qu'ils font est bien... Il y a aussi parfois tout simplement de l'indifférence. Plus grave est la démission. Elle se traduit soit par la simple résignation, celle de ceux qui pensent que tout a été fait et, qu'hélas, notre pays va perdre peu à peu, ses savoir-faire et n'a plus aucune capacité à se développer ; soit par une posture idéologique de certains, pour qui la France serait sur le déclin, en tant que culture et modèle économique, et qui sur ces prémisses font plus confiance au soft power d'autres pays, réputés plus forts, qu'au leur.

Eh bien, je crois que les démissionnaires quels qu'ils soient ont tort ! Il y a un renouveau très perceptible. Nous avons toutes les expertises. Il nous faut maintenant les mettre en musique. Et c'est ce à quoi, modestement, la Délégation interministérielle à l'intelligence économique (D2IE) va s'employer dans les domaines qui sont les siens.

Eh bien, je crois que les démissionnaires quels qu'ils soient ont tort !
Il y a un renouveau très perceptible.

➔ RETOUR AU SOMMAIRE

Quels sont les points forts qui constitueront la politique publique que vous souhaitez mettre en œuvre ?

Nous devrons tout d'abord mieux anticiper les grands défis qui toucheront notre économie et nos entreprises. Ils sont internationaux, et technologiquement la plupart d'entre eux ont le fil conducteur commun du numérique. Mais surtout, il faut penser ces évolutions technologiques, les préparer et inventer de nouveaux modèles pour les mettre en œuvre. Rappelons-nous Al Gore utilisant la métaphore « des autoroutes de l'information », peu avant les années 1980, pour désigner ce qui allait devenir l'Internet d'aujourd'hui. Cette vision s'appuie sur la recherche prospective et la capacité d'influence des think tanks. Il s'agit en fait d'avoir une longueur d'avance afin d'agir en amont, sur notre environnement, en saisissant les opportunités et en structurant autant que possible notre « terrain de jeu » en fonction de nos propres intérêts, c'est-à-dire les règles, normes et bonnes pratiques. Notre deuxième force est celle de notre réseau, que nous devons apprendre à mobiliser et utiliser. Le décret du 22 août 2013 donne nettement des possibilités en ce sens à la D2IE. Cela concerne l'échelon central, en interministériel, comme celui des territoires et de nos représentations à l'étranger.

Je souhaite une D2IE à la fois stratège et experte en ingénierie d'intelligence économique. Enfin, je souhaite travailler dans l'esprit d'une administration de mission, réactive, en mode projet.

Je souhaite aussi accroître la lisibilité du dispositif public d'intelligence économique afin que les entreprises et les administrations sachent rapidement à qui s'adresser lorsqu'elles en ressentent le besoin, tant au niveau national que régional. Je pense en particulier à tous ces entrepreneurs qu'il ne faut pas décourager par trop de lourdeur. Parfois le mieux est l'ennemi du bien. Essayons d'abord d'être simples. Revenons aux fondamentaux de l'IE : veille stratégique et anticipation, sécurité économique, notamment immatérielle, influence et pédagogie. **Je souhaite une D2IE à la fois stratège et experte en ingénierie d'intelligence économique. Enfin, je souhaite travailler dans l'esprit d'une administration de mission, réactive, en mode projet.**

De quels leviers disposez-vous pour élever cette politique au rang des priorités de l'Etat et de l'ensemble des acteurs économiques ?

Un premier levier est celui donné par notre texte constitutif, le décret d'août précité, qui rattache directement la D2IE au Premier ministre, ce qui est un progrès important par rapport à la situation antérieure. Le deuxième repose sur la volonté dont je parlais plus haut, et que je sens concrètement sur le terrain, de changer d'état d'esprit. Il faudra que les échelons décisionnels écoutent ces aspirations qui sont le levain de notre succès économique futur. Enfin, il y a une vraie volonté politique, au sens le plus large et le plus noble du terme, d'essayer d'affronter différemment les défis. Ce sera ma tâche de porter cette bonne parole un peu partout auprès des acteurs divers, y compris privés, pour agir.

Quels sont selon-vous les cibles prioritaires des formations et sensibilisations à l'intelligence économiques ?

Il y en a plusieurs. D'abord travaillons pour le futur, c'est-à-dire formons les étudiants d'aujourd'hui. **Je considère indispensable que chacun sorte de l'enseignement supérieur en ayant reçu un enseignement de base en intelligence économique. Car finalement, l'IE c'est aussi la compréhension du monde, c'est l'analyse face au tout quantitatif, c'est l'anticipation et la réflexion active.** Il s'agit en fait des « nouvelles humanités », comme l'a dit un jour Eric Delbecque. Une expérience de diffusion de l'IE a déjà été lancée, il y a deux ans, dans une trentaine d'établissements. Nous devons encore l'évaluer mais je souhaite d'ores et déjà, l'étendre à un maximum de lieux de l'enseignement supérieur. Pour cela il nous faut convaincre le monde académique. Tous les étudiants devront, à terme, être formés aux notions de base de l'intelligence économique, quel que soit leur cursus. Mais il faut aussi irriguer les décideurs actuels qui

n'ont pas encore adhéré à cette approche. Comme c'est déjà le cas pour la sécurité au travail sur laquelle les salariés sont bien formés, il faut que la sécurité économique de l'entreprise, puis la veille deviennent l'affaire de toutes et de tous. L'influence, démarche proactive et aboutissement de l'IE, viendra naturellement ensuite.

Parallèlement, il est essentiel que les administrations centrales ainsi que les régions et départements forment leurs cadres, puis incitent les entreprises et centres de recherche à faire de même. **Il faut apprendre à mutualiser l'information utile à tous, au nom de l'intérêt commun de l'Etat, des entreprises, de la société civile. Finalement, c'est notre intelligence collective qu'il faut éveiller. L'un des objectifs de l'intelligence économique est bien de la stimuler en proposant des outils adéquats, et surtout des intervenants bien formés, car le défi c'est aussi la formation des formateurs.** Mon prédécesseur avait lancé le label Euclès avec l'INHESJ en matière de sécurité économique. Nous évaluons actuellement le système qui est intrinsèquement bon. Reste que cette démarche doit être initiée au plus haut niveau dans toutes les organisations, et que la valeur de l'exemple est, dans le domaine de l'IE, particulièrement essentielle. Il faut aussi tordre le cou aux a priori, aux idées toutes faites et aux images déformées de l'IE qui collent à notre domaine d'action. Afin de faire passer ce message et permettre une approche adulte de l'IE, j'ai commencé, et vais continuer, à me déplacer personnellement dans la France entière pour rencontrer les acteurs régionaux des administrations, des collectivités territoriales, des entreprises, les chercheurs ainsi que nos élus. Je suis à leur écoute, cherche à répondre à leurs demandes et leur présente notre expertise, qui est à leur service.

> Je considère indispensable que chacun sorte de l'enseignement supérieur en ayant reçu un enseignement de base en intelligence économique. Car finalement, l'IE c'est aussi la compréhension du monde, c'est l'analyse face au tout quantitatif, c'est l'anticipation et l'a réflexion active.

Concernant l'information et la sensibilisation à l'intelligence économique, la D2IE a déjà produit des documents, dont le Guide de l'intelligence économique pour la recherche, et va bientôt mettre en ligne, sur notre site, des fiches de sécurité économique adaptées à chaque cas. Nous élaborons, par ailleurs, des Principes directeurs pour les chercheurs en mobilité, ces derniers étant particulièrement concernés par ces problématiques.

Quels sont le principaux axes forts sur lesquels doivent reposer la construction d'une véritable stratégie d'influence à la française ?

Il s'agit d'un côté d'influencer l'environnement économique local pour orienter et soutenir les PME, qui détiennent un savoir-faire stratégique, en alertant sur des investisseurs prédateurs, en suggérant des orientations vers des marchés du futur, en suscitant la réunion, l'échange d'informations et l'action d'acteurs locaux.

Il s'agit aussi de préparer les marchés extérieurs à long terme. Qu'il s'agisse de régulations européennes et internationales ou de réputation, une influence professionnelle nécessite une information fine et en amont. Notamment sur les menées concurrentielles et sur les alliances possibles, sur l'élaboration de positions communes entre acteurs français, ce qui demande au préalable, un travail sur les idées, et sur l'image, ainsi que sur la capacité à animer des réseaux humains au sein et au-dehors des institutions concernées. Le tout sur des sujets liés aux besoins des acteurs économiques, de l'économie et des emplois futurs et en nous appuyant sur les fondamentaux culturels de la France.

Idéalement, la D2IE doit pouvoir exercer des alertes sur les influences extérieures en amont, apporter des informations utiles à la négociation, aider à la mise au point de positions communes entre acteurs, et également améliorer l'image et le suivi des actions. ■

Par **Eric DELBECQUE**
Chef du département sécurité économique de l'INHESJ

Relevons le défi de la guerre économique

Article publié dans *Le Monde* du 31 Octobre 2013 : http://www.lemonde

La NSA écoute la planète entière et espionne tous les grands dirigeants de ce monde : voici qui n'a rien d'une nouvelle fraîche pour tous les experts de l'univers de la sécurité nationale... On parle aujourd'hui de Prism, alors que l'on désignait auparavant le système d'écoute américain par le nom d'Echelon ; c'est tout ce qui a changé : un nom, et l'ampleur du phénomène. Comme l'expliquait très récemment Jean-Jacques Urvoas, cela ne veut pas dire pour autant que nous devons accepter de devenir des « victimes consentantes ». Et cela renforce précisément la nécessité d'une politique de légitimation du renseignement dans la stratégie de puissance nationale et européenne. Laquelle peut s'inscrire dans un cadre éthique (de respect des libertés individuelles) sérieux et crédible.

Pourquoi tant d'émotion alors ? Parce que cette affaire rend manifeste ce que beaucoup d'Européens ne souhaitaient pas voir en face, à savoir que les Etats-Unis nourrissent une conception du monde hégémoniste et unipolaire qui ne fait plus aucune distinction entre les notions d'alliés, de vassal et de rival. Il lui paraît donc totalement justifié de traiter les démocraties de la même manière ou presque qu'ils traitent leurs adversaires. On remarque d'ailleurs que c'est notre indignation qui les étonne... Washington ne tente même plus de dissimuler que le gouvernement américain place sa souveraineté très au-delà de celle des autres.

Indéniablement, l'espionnage, y compris économique, constitue une pratique de tous les Etats. En revanche, le Président Obama témoigne depuis le début de cette affaire d'un embarras extrêmement relatif ; certes, ces révélations apparaissent inappropriées et inopportunes mais elles ne provoquent aucune remise en question à la Maison Blanche. En fait, nous n'avons pas tiré toutes les leçons de la période Bush et de la petite phrase de Rumsfeld : « la mission détermine la coalition » !... Les Etats-Unis n'ont plus d'alliés « privilégiés » : ils construisent des partenariats révocables ou à géométrie variable. Mais ils ne sont pas les seuls : la Chine procède de la même façon. **L'Union européenne et les commentateurs des relations internationales semblent découvrir que les Etats poursuivent des intérêts, que les nations ne sont pas mortes et qu'il existe des jeux de puissance qui manipulent régulièrement les échiquiers économiques, qu'ils soient financiers, industriels ou commerciaux !...**

Ce qui nous apparaît également clairement grâce à ces « révélations », c'est que la lutte anti-terroriste n'est bien évidemment que l'une des raisons qui motivent la vaste entreprise de surveillance électronique américaine. L'espionnage économique s'avère essentiel. Ce système de quadrillage de la NSA recueille bien évidemment une quantité impressionnante d'informations industrielles, technologiques, financières, commerciales dont la communauté du renseignement d'Outre-Atlantique sait faire profiter les entreprises de l'Oncle Sam, d'une manière ou d'une autre. Le dispositif n'a rien de neuf puisqu'il fut mis

en place par le Président Clinton il y a vint ans ! Ce dernier avait en fait intégré dans la politique économique et industrielle de son pays un volet assumé de diplomatie des affaires (*Advocacy policy) et de renseignement économique !*

De nombreuses nations ont construit des dispositifs identiques, complétés par des politiques d'intelligence économique (laquelle s'inscrit quant à elle dans un cadre légal, contrairement à certaines des opérations des services de renseignement). La bonne question ne saurait donc être : pourquoi les « autres » nous espionnent pour faciliter leur dynamique de conquête de marchés ? L'excellente interrogation qu'il convient plus que jamais d'installer au centre de nos préoccupations économiques et géopolitiques est la suivante : pourquoi l'Europe en général et la France en particulier ne mettent-elles pas en place des mesures identiques à celles dont disposent les puissances commercialement offensives ?

Pourquoi ne tire-t-on pas toutes les conséquences d'un principe général de réciprocité ? *Soit nous nous battons à armes égales avec le reste des nations sur la scène de la grande confrontation géoéconomique planétaire, soit nous serons éternellement les dindons de la farce d'une idéologie libérale absolutiste, ou plutôt caricaturale, purement européenne, qui veut absolument appliquer en intégriste une « doctrine » qui se révèle régulièrement un masque. En effet, tous les Etats des autres continents savent parfaitement qu'elle est démentie quotidiennement : de multiples acteurs étatiques et industriels la violent en toute impunité.*

Il ne faut pas pour autant se satisfaire de ce climat de « guerre économique », d'hyperconcurrence ou d'hypercompétition (peu importe le mot que l'on préfère), qui baigne désormais les relations économiques internationales. ***Il est certes capital d'en prendre acte, de ne pas nier la réalité des rivalités géoéconomiques mondiales, de s'y préparer en conséquence sans reculer devant les révolutions culturelles que les affrontements de puissance génèrent, mais il faut travailler ardemment à construire la paix économique, ou plutôt les coopérations qui la fonderont ! Car ce modèle de commerce darwiniste des nations ne répondra jamais aux grandes questions du développement durable, de la promotion des droits de l'homme et d'un principe général de responsabilité, qui peuvent seuls fonder la sécurité internationale.***

Un nouvel Art de la Guerre

De Jean-François Phélizon, **Editions Nuvis,** 2013.

Par Nicolas Arpagian

On recense nombre d'officiers qui se piquent de vouloir transposer au monde des affaires leur connaissance de l'art militaire. On lira plus utilement le cheminement inverse que nous offre Jean-François Phélizon, directeur général adjoint de Saint-Gobain, dans son dernier ouvrage : *Un nouvel Art de la Guerre*. Comme il l'écrit avec justesse: « on avait coutume de dire que l'argent est le nerf de la guerre ; aujourd'hui, c'est moins l'argent que l'opinion qui est le véritable nerf de la guerre. On avait coutume de privilégier les actions de vive force ; aujourd'hui, ce sont plutôt des actions obliques qu'il s'agit d'inventer et de mettre en place ». L'auteur est un fin connaisseur de l'analyse stratégique, qu'il décortique avec minutie dans une dizaine d'ouvrages qui mêlent les références à la pensée chinoise aux exigences du jeu d'échec. Il fournit ici un tableau complet des menaces et risques qui visent les organisations étatiques et économiques. Et le champ des agressions possibles semble sans limite : « Plus les sociétés humaines deviennent marchandes, plus elles ont besoin de sécurité ». Au-delà des coups qui peuvent être portés aux entreprises, institutions ou citoyens, Jean-François Phélizon pointe les effets suscités par les réponses étatiques. Avec la tentation d'une société de surveillance par anticipation qui justifierait sa mainmise sur la population par un souci *a priori* légitime de prévention des attaques. « Les forces régulières tirent de grands avantages de l'extension de la notion de secret », constate-t-il. Dans une volonté de renforcer la sécurité des personnes et des biens, l'élément différenciateur semble plus que jamais résider dans la détention de l'information. Qui permettra d'assurer un *leadership* à une entreprise, un avantage stratégique dans une négociation ou des meilleures conditions financières dans une transaction. **Que l'on soit sur un champ de bataille ou dans les allées d'un conseil d'administration ou d'une salle de marché, c'est bien la connaissance qui fait la prospérité.** Qu'il s'agisse de protéger celle déjà acquise ou de la faire croître. Reste alors à savoir identifier ce qui sera cette donnée à valeur ajoutée. « La qualité d'une information n'est pas d'être publique ou secrète. La nature des secrets est plus diverse que la classification utilisée d'habitude par les institutions politiques et militaires. Tous les secrets ne se valent pas, et toutes les façons de cacher une information ne se valent pas. Entre ce qui devrait être su, ce qu'on laisse entendre, ce qu'on cache à demi et ce qu'on ne montre pas du tout, il existe une continuité qu'il s'agit d'administrer », prévient l'industriel.

Jean-François Phélizon connaît trop les arcanes du commerce international pour savoir qu'il serait contre-productif de formuler ses concepts stratégiques de manière obscure. C'est dans un style clair et concret qu'il livre au lecteur ses analyses nourries de sa pratique opérationnelle et de sa science livresque.

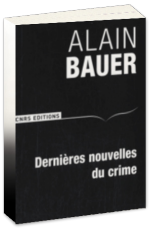
La société numérisée dans laquelle nous évoluons un peu plus chaque jour peut nous laisser croire à l'impérieuse nécessité d'accélérer continuellement nos échanges. Au point de limiter au minimum le temps de la réflexion et de l'analyse. « Dominer le temps consiste donc à rechercher l'anéantissement de l'adversaire, alors que jouer avec le temps consiste à rechercher l'attrition de ses forces avant d'envisager leur dislocation », avertit Jean-François Phélizon. Le temps consacré à la lecture de cet ouvrage fait assurément partie des préparations utiles à une meilleure compréhension du monde qui nous entoure.

Dans ses dimensions économiques, politiques mais aussi éminemment humaines.

L'ACTUALITÉ ÉDITORIALE

Dernières nouvelles du crime

BAUER Alain, **Paris, CNRS Editions,** octobre 2013



"Plus que jamais, le monde du crime fait preuve d'un génie de l'adaptation et de l'innovation. Reste aux professionnels de la lutte anticriminelle à faire preuve de la même créativité. **A. B."**

Quatrième de couverture

Géopolitique du terrorisme

DASQUE Jean-Michel, **Paris, Ellipses Marketing,** août 2013

Depuis les évènements du 11 septembre 2001, le spectre du terrorisme n'a pas cessé de hanter l'esprit des peuples et de leurs dirigeants.

Le terrorisme a des origines très anciennes mais il n'a pris de véritables proportions que dans la deuxième moitié du XIXe siècle avec les attentats des nihilistes russes et des anarchistes. La stratégie terroriste se caractérise par la recherche de l'effet psychologique, l'économie des moyens, la clandestinité, une gamme de cibles très ouverte et un élargissement de l'espace opérationnel. Aux entités solidement structurées, facilement identifiables, défendant des idéologies claires et souvent placées sous la dépendance de gouvernements étrangers ont succédé après la fin de la guerre froide des nébuleuses décentralisées, multiethniques, indépendantes du pouvoir politique et pratiquant une violence indiscriminée. Géographiquement les principaux centres de terrorisme sont concentrés dans un croissant s'étendant de l'Afghanistan jusqu'aux rivages de Sahel. Les États démocratiques ont renforcé leur coopération pour combattre le terrorisme mais ce dernier garde une capacité de nuisance.

Quatrième de couverture

➔ www.armand-colin.com

La France contre-attaque
Ces entreprises qui inventent le millénaire

BERGER Karine et RABAULT Valérie, **Paris, Odile Jacob,** septembre 2013

Ce livre entraîne le lecteur au cœur des entreprises françaises qui réussissent et qui innovent. Il nous dévoile ces PME qui exportent grâce à leur technologie et qui créent des emplois aux quatre coins du pays. Bref, il met le projecteur sur nos talents, si déterminants dans la compétition mondiale. Certes, cette bataille n'est pas encore gagnée. Et le danger serait de se tromper de combat en réduisant l'entreprise à un équilibre comptable et le profit à une stratégie de coût. Alors que c'est la création de valeur – véritable source de croissance – qu'il faut mettre au centre de notre politique économique. Avec un optimisme salutaire, Karine Berger et Valérie Rabault dessinent une stratégie globale et formulent des propositions – du financement à la transformation de l'environnement des entreprises – pour que la France réussisse sa contre-attaque.

Députée des Hautes-Alpes depuis 2012, Karine Berger a occupé différents postes de macroéconomiste, d'une part au ministère de l'Économie et des Finances, puis dans un groupe international dont elle a dirigé le marketing mondial jusqu'en 2011. Elle est également secrétaire nationale à l'économie du Parti socialiste.

Députée du Tarn-et-Garonne depuis 2012, Valérie Rabault, ingénieure des Ponts et Chaussées, a exercé jusqu'à fin 2011 dans une banque d'investissement où elle a géré les grands risques de marché.

Quatrième de couverture

➔ http://www.odilejacob.fr

La rentrée de la 17 ème session nationale spécialisée

Les auditeurs **de la 17 ème session nationale spécialisée de l'INHESJ** se sont réunis le 25 septembre 2013. Ils ont été accueillis, à l'occasion de cette journée de rentrée, dans les locaux du constructeur automobile RENAULT par Jean-Marc BERLIOZ, directeur de la prévention et de la protection. Eric DELBECQUE chef du Département sécurité économique et le colonel Michel GOYA, directeur de recherche au CDEF, ont livré leurs analyses sur le leadership au sein du commandement militaire et en entreprise. Cet après-midi a été aussi un moment de cohésion entre nouveaux et anciens auditeurs de la précédente promotion.

- Inscrivez- vous dès à présent pour la Session 2014 -1015

➔ Renseignements et Inscription

Nos publications

A paraître

- *Piraterie Maritime*, Philippe CHAPLEAU, Jean-Paul Pancracio, aux éditions Vuibert.
- *Les think tanks*, B. Huygues, aux éditions Vuibert.
- Déjà paru ➔ http://www.inhesj.fr

Colloques

- Les assises de la pensée stratégique novembre

  13 décembre 2013

➔ voir le programme détaillé

- La surveillance des maladies animales, un enjeu mondial de sécurité

  Colloque organisé par l'INHESJ le 18 décembre 2013

  SRAS, grippe aviaire, chikungunya, nouveau coronavirus... la plupart des agents pathogènes émergents pour l'Homme proviennent du monde animal. La mondialisation des échanges, associée au réchauffement climatique et à la demande croissante en protéines animales à l'échelle de la planète, conduit à une accélération significative de la circulation des agents infectieux et des risques de pandémies.

➔ http://www.inhesj.fr

- La sécurité au service de l'éthique

  jeudi 19 décembre 2013 à l'OCDE colloque annuel du CDSE

➔ Programme et inscription

Retours de conférences

De l'intelligence économique à l'intelligence juridique, La nécessaire protection du secret des affaires.

De l'intelligence économique à l'intelligence juridique, La nécessaire protection du secret des affaires. Cette journée d'étude organisée le 13 juin 2013 à la Cour de CASSATION visait à sensibiliser les magistrats aux problématiques de malveillance et de tentatives d'instrumentalisation de l'action judiciaire.
Eric Delbecque a introduit et modéré le panel de la matinée composé de Denis FORTIER, directeur de la rédaction de AEF -Sécurité globale, d'Alain JUILLET, senior advisor - ancien haut responsable à l'intelligence économique, de Rémy PAUTRAT, préfet de région honoraire, de Bernard CARAYON, avocat, ancien député, auteur du rapport "Intelligence économique, compétitivité et cohésion sociale" – 2003, de Claude REVEL, Déléguée interministérielle à l'Intelligence économique, de Jacques FOURVEL, conseiller du président du groupe Casino, président du comité de prévention des risques et de Jean-Luc MOREAU, global head product security de Novartis International AG.
Les actes de cette journée seront bientôt édités par la Cour de Cassation

Dans les médias

Prise d'otage à Nairobi

23/09/2013

Eric DELBECQUE

I TELE - Léa Seydoux

Fiction et Prospective - les 50 ans de France culture

09/09/2013

Eric DELBECQUE

France Culture - Les matinales

➔ http://www.franceculture.fr/player

Trophée de l'Intelligence Economique du 3 avril 2013

15/07/2013

Eric DELBECQUE

Newsletter n°9 L'essentiel de l'IESO - Paris Dauphine - Chaire Intelligence économique

➔ http://www.fondation.dauphine

Les géants d'Internet servent leur gouvernement avant leurs clients

08/07/2013

Nicolas ARPAGIAN

01Business - Opinions

5 questions sur les grandes oreilles de la DGSE

08/07/2013

Nicolas ARPAGIAN

➔ http://obsession.nouvelobs.com

Affaire prism Snowden est-il un nouveau Héro

02/07/2013

Eric DELBECQUE

France Culture TV - Matins de France Culture - Marc VOINCHET

➔ http://www.franceculture.fr

- Espionnage de l'UE: ce qu'il faut savoir sur l'arsenal de la NSA
  01/07/2013
  Nicolas ARPAGIAN
  L'Expansion - Raphaële KARAYAN
  → http://lexpansion.lexpress.fr

- Prism : sommes-nous tous sur écoute ?
  01/07/2013
  Nicolas ARPAGIAN
  France Info - Le Plus - Alice SERRANO
  → http://www.franceinfo.fr

- 01/07/2013
  Nicolas Arpagian
  AFP sur Dailymotion
  → http://www.dailymotion.com/

- Faut-il voir l'affaire Snowden à travers le Prism économique ?
  01/07/2013
  Nicolas Arpagian
  France Info - Clara Beaudou

- prism/espionnage américain
  01/07/2013
  Eric Delbecque
  I TELE - L'Edition du soir
  → http://www.itele.fr

- Espionnage des USA à l'encontre de l'U
  01/07/2013
  Eric Delbecque avec N.Arpagian, Nicolas Véron, Michel Fouquin,
  BFM Business - *« Les Décodeurs de l'éco » Fabrice Lundy*
  → http://http.mediacrawler.fr/

- "Affaire Prism"
  01/07/2013
  Eric DELBECQUE
  Radio classique - Le journal du business - Nicolas PIERRON

- La CIA vous surveille sur Facebook
  10/06/2013
  sur Nicolas Arpagian, l'auteur du Que sais-je? sur "la Cybersécurité"
  LCI soir sur Facebook
  → https://www.facebook.com/pages/LCI

- "la France crée sa cyberarmée"
  20/06/2013
  Nicolas Arpagian
  l'opinion - presse écrite N°130620

- "cyberguerre-nouveau-champ-bataille"
  08/05/2013
  Nicolas Arpagian
  bfm business TV - decodeurs-leco

- colloque ESSD organisé par le CSFRS
  30/05/2013
  sur intervention de Eric DELBECQUE
  Dépêche AEF - 9077

- "les hackers ont-ils reellement du pouvoir"
  21/05/2013
  Nicolas ARPAGIAN
  France Inter - le grand bain

- 30/05/2013
  Eric DELBECQUE
  Canal+ - Nouvelle édition

- 19/05/2013 - 01/05/2013
  Eric DELBECQUE
  I TELE - journal`

- 19/05/2013
  Eric DELBECQUE
  I TELE - La Matinale

- "Traque" du terrorisme sur Internet : "Une évidente nécessité"
  30/05/2013
  Nicolas ARPAGIAN
  Le Nouvel Observateur - Société- Celine RASTELLO
  → http://tempsreel.nouvelobs.com

- 01/05/2013
  Eric DELBECQUE
  - Hipotesis
  sur "sécurité privée enjeu public"
  Dépêche AEF- Sécurité globale n° 8982
  → http://www.infos-securitas.fr/questions-securite.php?archive=77

- « Pour les activités de veille et d'influence, je ne suis pas sûr qu'il faille légiférer »
  26/04/2013
  Eric DELBECQUE
  Dépêche AEF - 8860

- 19/04/2013
  Eric DELBECQUE
  I TELE - journal

- "en-temps-de-paix-la-guerre-est-elle-cyber"
  22/03/2013
  Nicolas ARPAGIAN
  sur France info
  → http://www.franceinfo.fr

- "quoi-pourrait-ressembler-pire-scenario-attaque-pirates-informatiques"
  13/03/2013
  Nicolas ARPAGIAN
  Article Atlantico
  → http://www.atlantico.fr

- "il ne peut y avoir de sécurité physique des infrastructures sans le volet numérique"
  13/03/2013
  Nicolas ARPAGIAN
  Dépêche AEF info - 8596

- Cyber-espionnage : "l'enjeu n'est pas d'empêcher 100% des attaques, mais de limiter leur impact"
  28/02/2013
  Nicolas ARPAGIAN
  La Tribune.fr - Informatique - Nabil Bourassi
  → http://www.latribune.fr

- "Données personnelles: comment Washington vous espionne"
  15/02/2013
  Nicolas ARPAGIAN
  Challenges.fr par Paul LOUBIÈRE
  → http://www.challenges.fr

- "La gestion de crise"
  01/02/2013
  sur "La gestion de crise", Laurent Combalbert et Eric Delbecque - Coll. Que sais-je ?, PUF, 2012, 127 p
  Alternatives Economiques - N° 321 - Marc MOUSLI

- 18/01/2013
  Nicolas ARPAGIAN
  LCI
  → http://www.wat.tv/

- Laurent Combalbert et Éric Delbecque publient
  04/01/2013
  sur "la gestion de crise dans l'entreprise", dans la collection « Que sais-je ? »
  Dépêche AEF info - n° 8029

→ RETOUR AU SOMMAIRE

INHESJ – Département Sécurité économique

Responsable éditorial : André-Michel Ventre

Directeur de la rédaction : Eric Delbecque

Rédactrice en chef : Diane de Laubadère

Site internet de l'INHESJ : www.inhesj.fr