

De l'intelligence économique

à la sécurité des systèmes d'information

par RÉMY FÉVRIER

L
E

développement des technologies de l'information et la multiplication des réseaux de diffusion ont accru la vulnérabilité des entreprises, quelles que soient leur taille et leur activité. L'intelligence économique doit donc devenir opérationnelle et faire partie intégrante des stratégies conduites par les acteurs économiques. La sécurité de leurs systèmes d'information doit désormais être au cœur des préoccupations afin d'assurer leur pérennité économique.

Les atteintes aux systèmes d'information des entreprises constituent de plus en plus une "voie royale" de déstabilisation directe ou indirecte. Au-delà d'une approche purement technicienne, la Sécurité des systèmes d'information (SSI) doit être envisagée en tant que composante intrinsèque d'une

intelligence économique opérationnelle. Elle doit ainsi pouvoir être directement mise en œuvre par les entreprises, indépendamment de leur taille ou de leur secteur d'activité. La complexité croissante des environnements économiques et sociétaux, catalysée par la diffusion des nouvelles technologies de l'information, a conduit à la vulnérabilité accrue des acteurs économiques. Pour ces entreprises, conscientes de l'obsolescence de leurs anciens modes de réflexion, le recours à l'intelligence économique est une nécessité plus qu'un choix.

Devant l'absence de définition universellement acceptée de l'intelligence économique, nous retiendrons celle proposée à l'occasion de l'élaboration du rapport du Commissariat général au plan, intitulé *Intelligence économique et stratégie des entreprises* (1994), dit

DOSSIER

DE L'INTELLIGENCE ÉCONOMIQUE À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

(1) Disponible en version intégrale sur le site de la Documentation française : <http://lesrapports.ladocumentationfrancaise.fr/BRP/074000410/0000.pdf>

rapport Martre⁽¹⁾. Ce dernier décrit l'intelligence économique comme

« l'ensemble des actions coordonnées de recherche, de traitement, de distribution et de protection de l'information utile aux acteurs économiques, obtenue légalement ». Même si depuis, elle a fait l'objet de nombreuses variantes, cette définition aborde néanmoins trois aspects fondamentaux : la grande diversité des actions constitutives d'une démarche d'intelligence économique, les apports

d'une telle démarche en termes de stratégies d'entreprise et son caractère exclusivement licite.

Émergence de l'intelligence économique

Certains États, à la vocation maritime affirmée (République de Venise, Ligue

(2) La Hanse, Ligue hanséatique, Hanse germanique ou encore Hanse teutonique est l'association des villes marchandes de l'Europe du Nord autour de la mer du Nord et de la mer Baltique. Elle prit naissance en 1241, par le traité formé entre Hambourg et Lubeck, dans le but de protéger leur commerce contre les pirates de la Baltique et de défendre leurs franchises contre les princes voisins. Les avantages que produisit cette union attirèrent progressivement un grand nombre de villes.

hanséatique⁽²⁾, Empire britannique...), furent les premiers de l'Histoire à mettre en place, assez naturellement, une politique d'intelligence économique. Celle-ci était fondée sur la simple idée que le partage et la circulation de l'information entre les différents acteurs

économiques étaient de nature à favoriser durablement leur développement économique. Ces novateurs furent tardivement rejoints, en 1950, par le Japon, qui devait assurer la reconstruction de sa compétitivité économique. Dans les années 1960, c'est au tour des États-Unis, où les grands groupes industriels se sont appropriés des pratiques issues du renseignement. Une tendance accrue depuis l'administration Clinton, qui a élevé le soutien aux entreprises nationales au rang de priorité gouvernementale. Pour autant, dans la grande majorité des cas, à l'exemple de



Sirpa gendarmerie - ADC F. Balsamo

La sécurisation des systèmes d'information contribue à la pérennité économique des entreprises.

l'Union soviétique, il a souvent fallu attendre l'effondrement d'un système et l'émergence d'un nouveau type de capitalisme hyperconcurrentiel, pour que les gouvernements prennent conscience de la nécessité de se doter d'une véritable doctrine de préservation de la compétitivité de leurs entreprises.

L'exemple français

En France, une première tentative de politique publique verra le jour en avril 1995, au travers de la mise en place d'un Comité pour la compétitivité et la sécurité économique. Celui-ci n'aura finalement qu'une existence éphémère. En dépit de la mobilisation d'une poignée de hauts fonctionnaires opiniâtres et de chefs d'entreprises convaincus, qui impulseront une véritable dynamique au travers d'actions locales, il faudra attendre 2003, et le choc psychologique induit par la prise de contrôle d'un des fleurons de la technologie française, la société *Gemplus*, par des fonds d'investissements anglo-saxons, pour qu'un parlementaire soit officiellement chargé de réfléchir spécifiquement au problème de la vulnérabilité des entreprises françaises. Cela donnera lieu au rapport de Bernard Carayon, député du Tarn. Intitulé *Intelligence économique, compétitivité et cohésion sociale*⁽³⁾, ce

(3) Disponible en version intégrale sur le site <http://lesrapports.ladocumentationfrancaise.fr/BRP/034000484/0000.pdf>

document provoquera une véritable prise de

conscience des faiblesses et vulnérabilités des entreprises françaises. Il sera en grande partie à l'origine de la mise en place d'une véritable politique publique nationale d'intelligence économique.

De 2004 à 2009, le Haut responsable à l'intelligence économique (HRIE), structure interministérielle placée sous l'autorité du Secrétariat général à la Défense nationale (SGDN), a constitué la pierre angulaire du dispositif national d'intelligence économique. Selon son ancien dirigeant, M. Alain Juillet⁽⁴⁾, « *la*

(4) Ancien directeur du renseignement de la Direction générale de la sécurité extérieure (DGSE) et ancien dirigeant de plusieurs grandes entreprises privées.

(5) <http://www.intelligence-economique.gouv.fr/>

politique publique d'intelligence économique est à la fois défensive et imaginative, légale et respectueuse des engagements de la

France, sans pour autant être naïve »⁽⁵⁾.

En six ans, le HRIE a ainsi mené un ensemble d'actions visant à promouvoir l'intelligence économique. De nature opérationnelle (conférences de sensibilisation) ou stratégique, elles ont conduit à la définition d'un nouveau périmètre de souveraineté nationale et à la protection des entreprises françaises victimes de tentatives de déstabilisation. Depuis le 17 septembre 2009, un Comité directeur de l'intelligence économique a vu le jour, placé auprès de la présidence de la République. Cette assemblée fixe les orientations du nouveau délégué

DOSSIER

DE L'INTELLIGENCE ÉCONOMIQUE À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION



Sirpa-gendarmerie - ADC F. Balsano

Les postes de travail et les serveurs des entreprises peuvent être la cible d'intrusions que quelques précautions simples et de bon sens peuvent prévenir.

est celui de la surinformation, il devient essentiel, non seulement de connaître précisément les besoins en informations de l'entreprise, mais également de disposer des outils et ressources nécessaires à leur recueil et leur

interministériel à l'intelligence économique, lequel « *élabore et propose la politique publique d'intelligence*

économique. Il en anime et coordonne la mise en œuvre et en évalue l'efficacité »⁽⁶⁾.

(6) Décret n° 2009-1122 du 17 septembre 2009 relatif au délégué interministériel à l'intelligence économique.

(7) Décret du 1^{er} octobre 2009 portant nomination du délégué interministériel à l'intelligence économique.

M. Olivier Buquen⁽⁷⁾, ancien élu et cadre dirigeant ayant exercé

au sein de plusieurs grands groupes privés, est le premier titulaire de ce poste.

Outils et concepts

Un certain consensus se dégage, qui considère l'intelligence économique comme étant structurée autour du triptyque : veille, sécurité économique et influence.

La veille d'abord, parce que le premier des préceptes de l'intelligence économique consiste en effet en la maîtrise de l'information stratégique indispensable à l'entreprise. Or, dans un univers informationnel global, où le principal risque

est celui de la surinformation, il devient essentiel, non seulement de connaître précisément les besoins en informations de l'entreprise, mais également de disposer des outils et ressources nécessaires à leur recueil et leur traitement. La sécurité économique ensuite, car le développement sans précédent de la compétition économique a poussé certaines entreprises à mettre en place de véritables politiques de déstabilisation de leurs concurrents, notamment en ayant recours à des campagnes de dénigrement déléguées à certains cabinets spécialisés. Des actions de communication offensives ont ainsi été dirigées contre des entreprises hexagonales de toutes tailles. Si le but recherché est variable, de l'élimination d'un concurrent trop performant à la tentative de prise de contrôle, le processus est toujours le même : la fragilisation de la cible au travers d'actions agressives coordonnées.

Enfin, l'environnement d'une entreprise étant devenu extrêmement complexe et changeant, les sociétés françaises doivent clairement s'inspirer du savoir-faire anglo-saxon en matière de *lobbying*, afin d'acquérir à leur tour une véritable "culture d'influence".

Sécurité des systèmes d'information et pérennité de l'entreprise

Les systèmes d'information constituent l'un des vecteurs majeurs de pénétration de l'entreprise et de captation de ses informations stratégiques. De fait, la SSI devient un enjeu majeur de sa pérennité. Longtemps considérés comme une simple fonction support de la chaîne de valeurs de l'entreprise, les systèmes

(8) Porter, M. 2003. *L'Avantage concurrentiel. Comment devancer ses concurrents et maintenir son avance*. Paris : Éditions Dunod - 647 pages

d'information sont désormais au cœur de l'activité économique et tendent à constituer une source d'avantage

concurrentiel indirect (au sens de M. Porter) (8).

Alors même qu'une gestion optimale des systèmes d'information de l'entreprise apparaît essentielle, rares sont encore les dirigeants de petites et moyennes entreprises à mettre l'accent sur leur sécurisation. Pourtant, les modes de captation des informations depuis les serveurs et postes de travail sont multiples et quelques précautions simples et de bon sens seraient de nature à considérablement réduire les risques encourus. Sans s'aventurer dans des détails techniques, on constate que les principaux risques liés à l'utilisation d'un système d'information se classent en trois grandes catégories : l'utilisation imprudente des postes de travail, les vols de portables et la pénétration directe des réseaux, filaires et sans-fil.

L'image institutionnelle d'une entreprise et de ses marques commerciales, fruit le plus souvent d'années d'efforts soutenus en matière de communication et de marketing, apparaît ainsi extrêmement vulnérable aux manigances de plus en plus agressives de la concurrence. Le détournement d'un site Internet constitue ainsi une arme nouvelle et redoutable, par exemple dans la lutte opposant des groupes de pression ou ONG à de grands groupes économiques au motif de leurs activités industrielles ou commerciales. Toutefois, si ce type d'attaques paraît le



Sirpa-gendarmerie - ADC F. Balsamo

Désormais, la volonté des tribunaux est de responsabiliser de plus en plus l'entreprise et donc ses responsables sur les problèmes de sécurité.

DOSSIER

DE L'INTELLIGENCE ÉCONOMIQUE À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

plus souvent limité à des enjeux médiatiques et sociétaux propices à la polémique, il n'en demeure pas moins que n'importe quelle entreprise, indépendamment de sa taille ou de son secteur d'activité, peut être victime de campagnes de dénigrement au travers de la violation de son S.I.

La mise en cause de dirigeants, relativement à une sécurisation insuffisante de leur S.I., constitue une autre menace possible. La volonté des tribunaux est de responsabiliser de plus en plus l'entreprise et donc ses responsables sur les problèmes de sécurité. On ne s'intéresse pas seulement à la faute, mais aussi aux personnes qui auraient pu l'empêcher. Le but est d'encourager les dirigeants d'entreprise à prendre conscience du caractère indispensable que revêt aujourd'hui la sécurité des S.I. et à utiliser l'ensemble des ressources à leur disposition afin de les sécuriser, faute de quoi ils peuvent être directement mis en cause.

Au-delà de la recherche d'une sécurité économique optimale, le caractère singulièrement récurrent de l'absence de prise de précautions au sein des entreprises françaises, en termes de sécurisation de leur système d'information, corrélé au nombre et à la diversité des menaces potentielles, fait que l'entité économique, soucieuse de protéger son S.I., dispose, dans les faits, d'un avantage concurrentiel indirect

susceptible, non seulement de lui permettre de pérenniser son activité en cas de crise majeure, mais également d'éviter certaines mises en cause médiatiques extrêmement préjudiciables. Toutefois, un tel objectif n'est envisageable qu'au travers de la définition et de la mise en place d'une véritable politique de sensibilisation à destination de l'ensemble des salariés de l'entreprise. À défaut, tout effort en matière de réduction des risques de pertes d'information stratégiques demeurera vain.



RÉMY FÉVRIER

Chef d'escadron Rémy Février, officier de gendarmerie, affecté à l'état-major de la Région de Gendarmerie Nord-Pas-de-Calais.

Chargé de mission intelligence économique et commissaire général délégué du Forum International sur la cybercriminalité, il est également chargé d'enseignements à l'Université et auprès de grandes écoles.

Le chef d'escadron Rémy Février est diplômé d'une école supérieure de commerce, ainsi qu'en Science-Politiques, finances publiques et informatique. Il a par ailleurs été auditeur de l'Institut des hautes études de Défense nationale (IHEDN) et de l'Institut des hautes études de la sécurité intérieure (IHESI).