La lettre d'Intelligence Économique et Territoriale de l'EM Normandie – N°22

Comprendre & Entreprendre

Se développer dans un monde complexe

La criminologie à la rescousse des territoires : l'urgence du renseignement économique

Alain Bauer

L'impact médiatique du terrorisme ne doit pas occulter la montée en puissance des nouvelles menaces criminelles qui visent les forces vives de nos territoires, au premier rang desquelles les petites et moyennes entreprises. Figure de proue de la criminologie, professeur au CNAM (Conservatoire national des arts et métiers) et dans de prestigieuses institutions à travers le monde, Alain Bauer est un spécialiste international des questions criminelles et terroristes ainsi qu'un fin connaisseur de l'univers du renseignement.

Dans l'entretien qu'il a accordé à Jean-Guy Bernard, Directeur Général de l'EM Normandie, Alain Bauer explique les mutations culturelles auxquelles sont confrontées les entreprises françaises en matière de sécurité. Dressant un bilan lucide du renseignement français, il explique comment une combinaison harmonieuse entre le CNAM et les autorités françaises a permis que se crée en Bretagne la première école française dédiée à la formation aux métiers du renseignement. Avec en filigrane une question : à quand une filière grandes écoles dédiée spécifiquement au renseignement économique ?

En quoi les PME installées sur les territoires sont-elles concernées par la criminologie ? Comment les aider à prendre conscience des enjeux, quand on sait que des méthodes aussi éculées que la fraude téléphonique au Pdg fonctionnent encore ?

Il s'agit là avant tout d'un problème d'ordre culturel. Il suffit de prendre un TGV et d'écouter les conversations téléphoniques pour avoir très simplement connaissance - outre les sujets intimes - de projets industriels ou de négociations commerciales qui devraient, en toute logique, être d'ordre confidentiel. Nombre de nos contemporains s'imaginent qu'une *business* ou une première classe sont des endroits protégés qui ressemble à leur salon...

En outre, en France, il est très difficile de faire comprendre à un interlocuteur que quelque chose qui n'est pas encore arrivé va cependant se produire. La France est par excellence le pays du déni. Il suffirait ainsi de ne pas penser à un événement, de refuser même de l'envisager, pour avoir une chance que le dit-événement ne se produise pas ! C'est là du "*wishful tinking*" dans toute sa splendeur ! Aux Etats-Unis, c'est différent. On ne dit pas que ce n'est pas possible, on demande juste combien ça coûte. Ensuite s'établit une équation entre le budget nécessaire pour se préparer à l'épreuve envisagée et ce que ça va coûter si on ne fait rien. Il n'y a pas de débat philosophique sur la possibilité ou non que l'événement puisse survenir. Pragmatisme oblige !

En France, en matière criminelle, évoquer un précédent permet donc de gagner du temps. Ensuite, il est indispensable de montrer que la sécurité est un facteur de production comme un autre. Elle a sa place pleine et entière dans le processus de production. Et ce quelle que soit la taille, la localisation et l'activité de l'entreprise. Toute entreprise se trouve donc être concernée par les enjeux sécuritaires, y compris les micro-entreprises. Pour preuve, on ne compte plus le nombre de start-up avec des technologies de pointe qui pensaient n'intéresser personne et dont les brevets

Comprendre & Entreprendre

De par sa vocation, l'EM Normandie entretient un lien puissant avec son territoire et les entreprises qui s'y développent. D'où sa légitime implication dans les enjeux relevant de l'Intelligence Économique et Territoriale. Car c'est ici, sur notre sol, que s'enracinent les projets qui assureront demain notre prospérité.

La lettre de réflexion Comprendre & Entreprendre vise à soutenir cette dynamique. Elle s'adresse à toutes celles et ceux qui anticipent, imaginent l'avenir et doivent faire des choix stratégiques. Seule la combinaison astucieuse de l'action et de la réflexion nous permettra d'optimiser notre positionnement et notre engagement au sein d'un monde complexe et mouvant.

ou savoir-faire ont été pillés sans vergogne. Les exemples de ce type sont légion. Malheureusement, ils entrent le plus souvent dans la rubrique des faits divers, sans que la presse économique ne traite jamais – ou presque – de ces questions. Le criminologue se trouve donc dans la logique de l'assurance-incendie. Nul ne prend une assurance de ce type pour que sa maison ou sa voiture brûle ! On le fait "au cas où". D'où la nécessité pour le criminologue d'expliquer les choses logiquement, par un *process* de déduction, en désacralisant la question sécuritaire. Prenez l'exemple de la ceinture de sécurité en voiture. Il y aura toujours des gens pour ne pas appliquer cette précaution. Mais c'est là un phénomène résiduel. Et la sécurité est assurée.

Inconscience, incompétence, paresse, crédulité, bêtise... les portes par lesquelles les hackers entrent dans nos systèmes résident avant tout en l'humain.

Dans l'entreprise, il en va de même. Globalement, les directeurs de sécurité des grands groupes sont maintenant bien formés. Il faut donc désormais amplifier ce cercle vertueux en direction des ETI et des PME, au coeur des territoires. C'est là qu'il nous incombe de former et de sensibiliser des cadres dont la sécurité ne sera pas la tâche principale, mais qui auront cette compétence dans leur spectre d'activité, et donc une capacité d'alerte et de vigilance. Ainsi, au sein du CNAM, nous allons mettre en place, au profit des formations RH, des modules spécifiques consacrés à la gestion des *process* de radicalisation en entreprise. Et ce, à la demande expresse d'un certain nombre de DRH.

En matière de menaces criminelles, on a affaire, dans la quasi-totalité des cas, à de l'escroquerie classique, parée des atours du cyber. Les criminels n'inventent quasiment jamais rien, ils recyclent de l'existant.

Enfin, pour revenir à votre question concernant la fraude au président, on doit relever que ce type d'arnaque, visant des extorsions de fonds, cible – là aussi pour des raisons culturelles – essentiellement le marché français. Nous avons malheureusement un fonctionnement quasiment impérial de l'entreprise. Aussi, les subalternes vont exécuter l'ordre émanant du grand patron (dont ils croient reconnaître la voix au téléphone) au lieu d'appliquer les procédures. Il faut d'ailleurs bien se rendre compte que dans la quasi-totalité des cas de ce type, la faille est humaine et requiert la participation de la victime. Regardez avec quelle facilité le compte de campagne d'Hillary Clinton a été piraté lors de la présidentielle américaine ! C'est là le niveau le plus banal du hacking. Il leur a été demandé tout simplement de changer un mot de passe, sans qu'ils prennent la peine de s'enquérir de l'origine de la dite-demande, sans même en référer à des experts en sécurité informatique…

Bref, inconscience, incompétence, paresse, crédulité, bêtise… les portes par lesquelles les hackers entrent dans nos systèmes résident avant tout en l'humain. En réalité, très peu d'opérations de hacking – 1% – sont réellement techniquement sophistiquées, requérant des moyens "lourds". Il s'agit alors souvent d'opérations émanant d'Etats ou d'entités agissant pour leur compte. Mais ces cas sont l'exception, non la règle.

L'impact des attaques terroristes a-t-il joué sur la prise en compte des paramètres sécuritaires au sein des entreprises ? Comment faire comprendre aux PME et aux collectivités territoriales que la dimension internationale des activités criminelles peut aussi les concerner et donc les atteindre dans leur quotidien ?

Depuis 2001 aux Etats-Unis et 2015 en France, l'impact médiatique du terrorisme fait que la question sécuritaire ne peut plus être balayée d'un simple revers de la main. La place du directeur de la sécurité a fortement évolué, même s'il reste encore beaucoup à faire. On voit d'ailleurs aujourd'hui des start-up se saisirent de la question dès leurs premiers pas. Elles savent, par exemple, qu'il leur faut être reconnues par l'ANSSI (Agence nationale de la sécurité des systèmes d'information), avec des process validés. Cette évolution des comportements a pour corollaire une appréhension plus lucide de la question. Plus besoin de passer des mois à convaincre l'interlocuteur qu'un attentat ou une attaque cyber sont à envisager… Le nombre considérable de petites sociétés victimes de tentatives d'extorsions d'argent suite à des attaques cyber prouve que chacun est désormais concerné.

En fait, en matière de menaces criminelles ou terroristes, ce qui apparaît comme nouveau, c'est tout simplement et le plus souvent ce que l'on a oublié. La technologie permet juste que l'on aille plus vite et plus loin. Sitôt connecté à internet, chacun sait que les opportunités comme les menaces peuvent venir de partout. Pour avoir une idée de "l'état de l'art" en matière de cybercriminalité et d'arnaques diverses, année après année, on peut se reporter aux analyses menées par le Clusif (Club de la sécurité de l'information français). Dans la quasi-totalité des cas, on a affaire à de l'escroquerie classique, parée des atours du cyber. Les criminels n'inventent quasiment jamais rien, ils recyclent de l'existant. Face à de telles menées, là encore, il faut faire de la pédagogie à partir d'exemples concrets et ne pas hésiter à citer des individus ou des entreprises qui se sont fait gruger. Souvenons-nous qu'un bon cas d'école vaut mieux qu'un long discours. Rien ne vaut l'expérience. C'est pourquoi mes cours de criminologie sont toujours accompagnés de plusieurs centaines de liens décrivant des cas concrets venant à l'appui de mes démonstrations. Ainsi, chacun peut faire son miel de l'expérience d'autrui. Si c'est déjà arrivé, c'est que ça peut se reproduire. Il faut faire en criminologie de la science-réalité comme existe la télé-réalité.

Quelle est votre perception de l'évolution des services de renseignement ? Le rythme des transformations est-il pertinent ?

Le renseignement est en fait formé de trois métiers. Tout d'abord, la collecte, où nous excellons, au point d'être d'ailleurs submergés de données. Ensuite l'analyse, où nous avons longtemps été défaillants. Enfin, l'action. Second élément à prendre en compte : le renseignement, ce sont aussi deux cultures différentes. L'une vient du contre-espionnage. Elle se déploie sur le temps long, avec patience, dans une logique de réseau à remonter, le tout nécessitant un secret absolu pour protéger ses sources… L'autre culture est celle de l'antiterrorisme, dont la logique est exactement inverse. Le temps est court, il faut partager les informations et agir avant que l'attentat ne soit commis. Aussi, un même service de renseignement ne peut simultanément être en charge de ces deux métiers, qui ont des paramètres de fonctionnement si dissemblables, à moins de transformer les fonctionnaires en parfaits schizophrènes !

En outre, on sait que l'homme a par nature tendance à reproduire ce qu'il sait faire. Le renseignement n'échappe pas à la règle. L'espion soviétique a été l'alpha et l'oméga du renseignement occidental pendant un demi-siècle au moins. C'était facile et concret. L'apparition du terrorisme islamique est venue bouleverser la donne. Déjà lorsqu'en 1968, Raymond Marcellin arrive au Ministère de l'Intérieur (il y restera jusqu'en 1974), il a du mal à faire adopter par la DST (direction de la surveillance du territoire, contre-espionnage, ancêtre de la DGSI) la mise sur pied d'un service antiterroriste. D'ailleurs, même contrainte, la DST a du mal à s'y faire. Les Renseignements généraux, bien que fortement ancrés dans les territoires, n'y croient pas non plus et ne perçoivent pas la monté en puissance du terrorisme non politique (ni 1983, ni 1986, ni 1995...). Longtemps, nos services vont être désemparés, d'abord parce qu'ils ne cernent pas correctement le problème. Ils arrivent certes à arrêter les terroristes après le passage à l'acte, mais pas à prévenir leurs frappes.

Aujourd'hui, le renseignement français a su peu ou prou s'adapter à cette réalité complexe, ce qui le force à une révolution non pas tant structurelle que culturelle. En leur temps, Michel Rocard et Rémy Pautrat l'avaient compris. Il faudra en réalité vingt ans pour que leur plan entre en application… sous Nicolas Sarkozy, puis sous Manuel Valls et Bernard Cazeneuve. Sous les coups de boutoir des récents attentats, une relance s'est opérée. Globalement, une évolution positive se dessine, puisque de plus en plus de terroristes font l'objet d'arrestations préventives, autrement dit avant d'être passés à l'acte. Les services dans leur ensemble sont davantage proactifs et peu à peu parviennent à anticiper. Ces progrès sont indéniables. Nous sommes en train de rattraper notre retard, même si l'on sait bien que l'on ne peut tout prévenir en matière terroriste. Soyons justes, même les Américains avec leurs puissants moyens ne sont pas parvenus à prévenir les attentats de 2001. C'est la preuve que la révolution culturelle que j'évoque ici doit donc être conduite non seulement en France mais bien dans l'ensemble du monde occidental.

Avec l'intensification du risque terroriste, ne risque-t-on pas de voir nos services baisser la garde dans le domaine de l'intelligence économique ?

Le renseignement est en fait formé de trois métiers : la collecte, l'analyse et l'action.

Il est vrai que l'impact médiatique généré en France par les attaques terroristes a conduit les autorités à parer au plus pressé. Mais ne négligeons pas pour autant la dimension que vous évoquez. D'autant que les questions économiques ont toujours été au cœur de l'activité des services de renseignement américains. Les Etats-Unis sont un pays pragmatique. Leur problème essentiel est de tuer la concurrence et de favoriser l'innovation. C'est le seul pays où, deux fois par an, se tient une conférence où les principaux directeurs des services de renseignement et de sécurité des entreprises rencontrent les services fédéraux, lesquels sont là pour les aider. Une telle attitude est impensable en France où l'on considérerait cette proximité comme un dévoiement du service public ! Là aussi, une authentique révolution culturelle est à accomplir, malgré les efforts récents à souligner.

En vérité, en France, que ce soit en matière de découvertes technologiques ou de start-ups à soutenir, c'est moins le renseignement qui fait défaut que l'adoption d'autres paramètres, d'ordre financier par exemple. Ainsi, lorsque nous soutenons des start-up, a-t-on la capacité de contrôler leur devenir ? L'un des tropismes de Bercy n'est-il pas de se focaliser sur les seuls fleurons du CAC 40 et parallèlement, son incapacité à voir à petite échelle ? Plus généralement, l'un des défauts majeurs de notre pays n'est-il pas de penser qu'il incombe à l'Etat de s'occuper de tout ? Bref, que ce soit en matière de renseignement *stricto sensu* ou de guerre économique, c'est bien avant tout le pragmatisme qui nous fait défaut.

Les questions économiques ont toujours été au coeur de l'activité des services de renseignement américains. Les Etats-Unis sont un pays pragmatique. Leur problème essentiel est de tuer la concurrence et de favoriser l'innovation.

En matière de formation au renseignement, la France n'a-t-elle pas pris un retard important ? Pouvez-vous nous parler des initiatives qui ont été prises en France par vous-même et différentes autorités dans le cadre du CNAM pour remédier à cet état de fait ? *Quid* de la situation en France au regard du monde anglo-saxon que vous connaissez bien ?

Ce n'est que tout récemment, depuis deux ans, que, dans le cadre du CNAM, la France s'est dotée d'une école spécialisée, localisée en Bretagne, initiative

lancée avec l'accord de quatre services français et de deux ministères. Maintenant, en partenariat avec les ministères de la Défense et de l'Intérieur, le pôle CNAM Sécurité Défense permet à des étudiants ou à des professionnels de suivre, sur la Technopole de Saint-Brieuc Armor, durant une année universitaire, un cycle de formation hautement professionnalisant offrant des débouchés directs dans les services de l'État ou dans des entreprises à l'international. Et ce sans oublier des formations continues spécialisées, au niveau master, pour les personnels des services. Nous comptons aujourd'hui 90 élèves en licence et un peu plus de 70 en master.

Bref, nous avons mis sur pied un outil dont l'université française ne voulait pas vraiment. On trouve bien sûr çà et là dans le monde académique des formations portant sur le renseignement (et je salue le courage et l'abnégation de mes collègues), mais rien qui ne corresponde. Ce qui, somme toute, s'avère être très français, puisque nos "élites" considèrent le plus souvent avec condescendance – voire carrément avec mépris – cette profession, laquelle est au contraire perçue, sous d'autres cieux, comme un métier de "seigneurs".

Cette différence d'appréciation n'est pas anodine. Nos amis britanniques, par exemple, ont compris depuis longtemps l'importance de la formation au renseignement.

En ce sens, l'initiative menée à Saint-Brieuc relève d'une configuration inédite dans notre pays, même s'il reste beaucoup à faire pour améliorer ce *process*. Ainsi, pourquoi les écoles de commerce n'envisageraient-elles pas de créer une filière intitulée "renseignement économique" ? Car les entreprises doivent se défendre, non contre l'Etat mais en complément de lui. Il faudrait mener une telle action de façon adaptée, en parallèle d'autres formations initiales et permanentes, avec par exemple des certificats pour les PME et TPE qui n'ont pas les moyens d'avoir un service dédié. Le terme "Renseignement économique" fait peur diront certains. Peut-être… Mais cela ne retire rien au constat. Il faudra bien un jour prochain se décider à appeler les choses par leur nom !

Pour en savoir plus :
- Sur les cursus proposés par le CNAM en matière de sécurité – Défense : http://cnamsecuritedefense.fr/
- Sur Alain Bauer : http://www.alainbauer.com/

Extrait : "*Souvent, en matière criminelle ou de terrorisme, paraît nouveau ce qui est simplement oublié. L'amnésie collective est aggravée par les flux médiatiques qui font de l'immédiateté une garantie de savoir. Quand tout va toujours plus vite, chaque nouvelle en effaçant une autre, l'hystérie de l'instant obscurcit la réflexion.*" (in *Les terroristes disent toujours ce qu'ils vont faire*, cosigné avec François-Bernard Huyghe, PUF, 2010, p.5)

Abstract

Criminology to the rescue of Territories: Economic Intelligence urgently called for

The impact terrorism has had in the media should not hide the emergence of new criminal threats which target the dynamic forces of our territories, with our SMEs being first in line. A figurehead in Criminology, a Professor at the CNAM (*Conservatoire national des arts et métiers*) and in prestigious institutions across the world, Alain Bauer is an international expert in criminal and terrorism issues as well as a connoisseur of the world of Intelligence.

In the interview he granted to EM Normandie's Director General, Jean-Guy Bernard, Alain Bauer explained the cultural transformation French companies are faced with as regards security. While making a lucid review of the French Intelligence Services, he explained how a harmonious collaboration between CNAM and the French Authorities allowed to create in Brittany the first school in France dedicated to training for Intelligence Functions. With as an underlying issue, the following question: when shall we have a *Grande Ecole* track that would focus specifically on Economic Intelligence?

EM NORMANDIE
Comprendre & Entreprendre
Une publication de l'EM Normandie
Directeur de publication : Jean-Guy Bernard
Illustration Rossana - ISSN en cours

Contact : Ludovic Jeanne - IDéT
EM Normandie 9, rue Claude Bloch 14052 Caen cedex 4
Tél. : +33 (0) 2 31 46 78 87
Courriel : idet@em-normandie.fr - www.em-normandie.fr

IDéT NORMANDIE

Notre vision de l'Intelligence Économique et Territoriale

Comment rétablir dans nos économies le sens du stratégique, réhabiliter le long terme, se protéger tout en se montrant innovant ? En conciliant veille et action, vision et pragmatisme, l'Intelligence Économique & Territoriale (IE&T) s'impose comme un levier de compétitivité. Ensemble cohérent de pratiques et de connaissances, l'IE&T aide les entreprises comme les territoires à se positionner, se défendre mais aussi anticiper et se développer. Agir avec succès exige d'éclairer l'action par une compréhension fine des marchés et des environnements. À cet égard, l'IE&T est l'affaire de tous. Car le sens des responsabilités de chacun décide du succès commun.

De fait, l'IE&T s'impose à la fois comme un mode d'action et un regard multidimensionnel, cherchant à comprendre la complexité du monde pour mieux la maîtriser. L'IE&T nous invite ainsi à redéfinir nos cultures organisationnelles, à revoir nos pratiques et nos méthodes. Rien ne se fera sans convergence entre acteurs publics et privés, sans l'adhésion de tous à un projet commun, enraciné dans un territoire. Face aux nouveaux défis, mêlant harmonieusement action et réflexion, l'IE&T constitue le socle des succès à venir.