

Éditorial

Les enjeux de la protection du patrimoine
par J.-M. Durand

_ 1

Les conséquences de l'insouciance en matière de protection des résultats de la recherche
par M.-P. Van Hoecke

_ 2

Le mal des mails
par J. Illand

_ 4

A qui profite le crime ?
par J.-L. Toffart

_ 5

ÉDITORIAL

Les enjeux de la protection du patrimoine

« Que vaut le CNRS ? » C'est la première question qui m'est venue à l'esprit en réfléchissant à cet éditorial car la sécurité doit être proportionnée aux enjeux. Mais cette question difficile va bien au-delà du cadre de ce bulletin et nous nous interrogerons plutôt sur ce qui a de la valeur au CNRS.

Un organisme de recherche a des biens matériels (immobilier, grands et petits équipements...). Mais ce sont ses biens immatériels qui font sa raison d'être, même si sa comptabilité, qu'elle soit privée et encore plus publique, ne sait pas vraiment les mesurer et les prendre en compte. Et, parmi ces biens immatériels, l'information est un patrimoine essentiel tant pour son contenu en soi de connaissances que pour ce qu'elle permet : la valorisation des résultats de la recherche, le partage et la diffusion des connaissances, le développement d'une capacité d'expertise et la formation des personnes. Le lecteur attentif pourra reconnaître, dans cette énumération, les objectifs attribués à la recherche publique par le code de la recherche. Il est possible d'ajouter la notoriété de l'organisme de recherche et de ses chercheurs ainsi que les moyens dont ils disposent.

Cette information patrimoniale est d'abord dans les têtes des hommes et des femmes. Mais, pour être traitée et produire tous ses effets, elle doit être stockée et gérée dans des systèmes d'information. Ceux-ci sont toujours plus complexes et interconnectés, et donc toujours plus vulnérables. Leur sécurité doit, en conséquence, être en permanence renforcée. C'est une condition indispensable à l'intégrité et la disponibilité de l'information pour les personnes autorisées à la connaître, et à sa confidentialité vis-à-vis des tiers. C'est bien entendu l'affaire de spécialistes mais c'est aussi l'affaire de tous car la vulnérabilité des systèmes d'information est d'abord une question de comportement de chacun dans la perspective d'une défense en profondeur.

J'espère que ce bulletin vous sera profitable. Je vous en souhaite une bonne lecture, une prise de conscience renforcée de la haute valeur de votre patrimoine et des convoitises qu'il génère, et une information mieux protégée.

JEAN-MARIE DURAND

Haut fonctionnaire de défense et de sécurité

Ministère de l'enseignement supérieur et de la recherche

<http://www.enseignementsup-recherche.gouv.fr/cid20302/haut-fonctionnaire-de-defense-et-de-securite-h.f.d.html>

« Sécurité informatique » s'en est allé... Vive la « Sécurité de l'information » !

Les temps changent, le monde évolue. A la création de ce bulletin, en 1994, les problèmes de sécurité ne semblaient pas venir du réseau Internet, alors dédié strictement à la recherche, mais des échanges de disquettes entre micro-ordinateurs. Le bulletin s'est donc appelé « Sécurité informatique » et traitait surtout des « codes malveillants ». Quand l'Internet s'est ouvert au monde économique, en 1995, la sécurité a changé de dimension. Le bulletin en a gagné un sous-titre, « Sécurité des systèmes d'information ».

Aujourd'hui la sécurité porte non plus sur « les systèmes » en tant que tel, mais sur « l'information » dont les besoins de sécurité ont été déterminés par une analyse de risque. La mode n'est plus aux « remparts imprenables » autour de « machines sanctuaires » mais à l'organisation d'une « défense en profondeur » qui permet la poursuite de l'activité, même en mode dégradé, après que des systèmes soient tombés ou des machines compromises. La sécurité n'est plus vue comme un « état » mais comme un processus qui se répare et s'améliore en permanence. Les instances internationales appellent cette approche un « Système de Management de la Sécurité de l'Information ».

... Et voilà pourquoi « Sécurité informatique » est devenu « Sécurité de l'information » avec une nouvelle maquette mais avec le même esprit pour satisfaire le même public.

Robert Longeon

Chargé de Mission SSI au CNRS

Les conséquences de l'insouciance en matière de protection des résultats de la recherche

Par Marie-Pierre Van Hoecke

Conseiller en charge de la protection du patrimoine scientifique auprès du HFDS/MESR
marie-pierre.vanhoecke@recherche.gouv.fr

De tous temps, les hommes se sont déplacés, parfois très loin de chez eux, pour aller apprendre un métier particulier, pour en acquérir les connaissances et en découvrir les ficelles.

► Partager l'excellence

Parce que l'expertise dans un domaine était souvent localisée géographiquement, parce qu'elle s'était développée grâce au génie de l'un ou de l'autre ou grâce à la présence d'une matière première, d'une particularité climatique ou géographique, il fallait aller la chercher là où elle se trouvait. Sous le règne de Charles-Quint, on allait à Gènes pour apprendre la finance chez les banquiers génois. Pendant tout le moyen-âge, la faculté de médecine de Montpellier, première université de médecine du monde occidental et héritière de l'illustre école de médecine créée en 1220, attirait les étudiants de tous les pays. De même qu'avant elle, le génie d'Avicenne a attiré auprès du maître, dont le Canon a grandement influencé la pratique et l'enseignement de la médecine dans le monde, nombre de médecins étrangers. On s'est aussi déplacé de très loin pour apprendre les techniques et, surtout, pour découvrir les secrets des savoir-faire. Les exemples sont légion, à toutes les époques et dans toutes les régions du monde, et ce, tant dans les domaines civils que militaires. L'excellence attire, l'excellence fait des émules, l'excellence doit se partager pour que la connaissance puisse se propager.

► La protection et la diffusion du secret

Depuis Prométhée, « le prévoyant », les humains ont toujours cherché à développer de nouvelles techniques ou à se les approprier. Le mythe de Prométhée, métaphore de l'apport de la connaissance aux hommes, est l'illustration même du double sens du terme « appropriation » :

s'approprier une technique ou une méthode signifie soit apprendre à l'utiliser, la faire sienne au sens de l'intégration dans son propre environnement, soit la faire sienne au sens de la possession d'un bien et du droit à son utilisation ou à sa cession ultérieure. Bien des techniques et des savoir-faire ont été, et sont encore, protégés par des secrets. Les problèmes se posent quand l'appropriation d'une technique se fait sans l'autorisation de son inventeur ou de son détenteur, car les conséquences peuvent être très lourdes.

Posséder un secret c'est posséder le pouvoir, à tout le moins une supériorité de classe. Dans l'Égypte antique, le secret de l'embaumement des corps a été longtemps réservé aux pharaons et à leurs proches. La diffusion d'un secret de fabrication d'une classe privilégiée vers les autres classes permet sa démocratisation. De même certains secrets de fabrication ou privilèges d'utilisation détenus par les militaires se sont démocratisés et sont passés dans le domaine civil. Tel est le cas des cartes précises de géographie, qui, d'ailleurs, restent le privilège des militaires dans beaucoup de pays.

Si certains domaines ont toujours été propices à la diffusion de la connaissance, d'autres se prêtent plus naturellement au secret. Les avancées dans les domaines qui touchent à la santé humaine, comme la médecine ou la chirurgie, ont toujours montré une tendance au partage et à la diffusion des connaissances, bien que cela soit moins vrai maintenant que l'économie du médicament met en jeu des sommes importantes.

En revanche, dans les domaines technologiques, notamment les technologies mili-

taires ou duales, il existe une culture du secret du savoir-faire. Plus étrange, dans le domaine de l'artisanat, principalement ce qui a trait à la parure des hommes, et celui de l'art, cette culture de la protection du secret existe aussi. Le secret du travail des textiles et celui des métaux précieux, entre autres, ont fait l'objet de toutes les convoitises pendant des siècles. Au quinzième siècle, les techniques innovantes des peintres flamands ont attiré de nombreux amateurs, tout comme, bien longtemps auparavant, les techniques d'embaumement.

► Les enjeux de la diffusion du secret

La diffusion inconsidérée d'un secret de fabrication ou d'une technique de pointe peut être lourde de conséquences, au niveau d'un pays, et ce sur deux axes principaux : le domaine économique et le domaine géopolitique.

Conséquences économiques : il est clair que le vingt-et-unième siècle a commencé sous l'égide de la course à l'innovation. Celui qui possèdera l'innovation la plus moderne dominera l'économie mondiale. Celui qui imposera ses standards imposera ses produits au reste du monde, dominera le marché mondial, et, transitivement, garantira ainsi ses emplois. Nos économies sont donc entièrement dépendantes de notre potentiel créatif. Détenir le secret de fabrication d'un produit ou le secret de préparation d'une matière première donne au détenteur un avantage certain. Ceux qui veulent utiliser ce secret sont obligés d'en passer par les conditions du détenteur, comme dans le cas de la détention d'un brevet. L'enjeu économique de la diffusion d'une technique innovante

peut être décrit de façon simple, voire simpliste : il s'agit du maintien de l'emploi local, du PIB et, transitivement et à moyen terme, du maintien de la capacité d'innovation locale.

Les conséquences économiques de la diffusion d'une technique peuvent être de deux niveaux :

- soit il s'agit de la propagation d'un savoir-faire vers une région du monde qui l'utilisera pour satisfaire ses besoins propres. On peut penser, par exemple, à la diffusion, sur certains continents, de médicaments fabriqués sans licence. Dans ces cas, le détenteur du savoir-faire (un brevet en l'occurrence) ne perd qu'un manque à gagner. Moralement, si ce n'est juridiquement, la position du pays qui fabrique « illicitement » les médicaments en question est défendable, en termes de santé publique et de vies humaines. On peut penser que ces démarches tiennent de l'aide au développement et de l'altermondialisme ;

- soit il s'agit de la diffusion vers un fabricant ou un pays qui l'utilisera pour conquérir le marché domestique du pays qui a produit l'innovation. Cette conquête sera d'autant plus facile que le coût de l'innovation ayant été payé par le pays

innovateur, le coût de fabrication sera plus faible.

On le voit, la propagation inconsidérée d'une technique innovante, peut produire des effets désastreux sur l'économie du pays qui a financé l'innovation.

Conséquences géopolitiques : les conséquences géopolitiques de la propagation mal maîtrisée d'une innovation technique, si elles sont moins évidentes et, surtout, moins courantes, sont tout aussi importantes et indispensables à considérer.

La première conséquence géopolitique à considérer est, bien entendu, l'utilisation à fins terroristes de l'innovation. Si, dans le domaine des recherches à application militaire directes, l'appréhension du risque d'utilisation à fins terroristes de l'innovation est triviale, il l'est moins, mais est tout aussi présent, dans les disciplines à applications duales, qui, elles, sont parfois difficiles à évaluer.

La deuxième conséquence géopolitique néfaste, que je voulais évoquer, s'inscrit en creux. C'est plutôt la conséquence du refus de propagation de l'innovation. Reprenons l'exemple du besoin mondial en médicaments. Une poignée de compagnies seulement possède la totalité des brevets et une poignée de pays possède la capacité à développer de nouveaux trai-

tements. Refuser à certains pays, parce qu'ils n'en ont pas les moyens financiers, le droit d'accès à des traitements, alors qu'il n'existe pas de traitement alternatif, représente un choix géopolitique lourd de sens. Il en est de même dans les disciplines qui interviennent dans l'alimentation humaine, telles que l'agronomie ou le traitement de l'eau, par exemple. Si, dans ces secteurs, certaines innovations doivent rester la propriété du détenteur des brevets, parce qu'elles sont des innovations de confort, d'autres innovations se doivent d'être partagées, quand elles permettent la survie de populations.

► Le rôle des chercheurs dans le processus

On le voit, il est difficile de tracer la frontière entre ce qui doit être partagé, parce que cela répond aux droits humains indéniables comme l'alimentation, l'eau potable ou le droit à l'éducation, et ce qui doit être protégé, parce que le pays qui en financé l'éducation, les recherches, l'environnement scientifique propice à l'activité intellectuelle des chercheurs, a le droit de profiter des retombées économiques de son investissement.

Le philosophe allemand, Hans Jonas, dans son célèbre ouvrage paru en 1979, « le

Deux exemples historiques de transfert de technologie, riches d'enseignement

► Exemple 1 : la sériciculture

Les soieries étaient des textiles connus et prisés dans le monde entier. En revanche, la science de l'élevage du ver à soie, dont la connaissance était détenue uniquement par la Chine, était un secret protégé par le pays tout entier. Il faut dire que la protection de ce secret était une affaire d'état ! En effet, était punie de mort toute diffusion de la moindre connaissance ou du moindre savoir-faire en matière de sériciculture ou toute aide à l'exportation de matière première, œuf ou ver à soie.

Ce secret était tellement envié, que tous les pays, voisins ou plus lointains, ont redoublé de ruse et de subterfuges pour s'approprier les techniques de la sériciculture. Des légendes racontent que des Coréens auraient exporté des vers à soie cachés dans un pinceau à calligraphie, pinceau d'ailleurs toujours exposé dans un musée en Corée du Sud. D'autres légendes disent qu'une princesse chinoise, promise à un prince indien, aurait caché un ver à soie dans sa chevelure pour emporter avec elle des vers à soie, tant elle avait besoin de sa chère soie. La façon dont le Japon s'est procuré la technique a consisté en un vol de quelques œufs et ... de quatre ouvrières chinoises ! Même les moines chrétiens se sont damnés, en emportant, caché dans leur bâton de pèlerin, des vers à soie à destination de l'empereur Justinien en 552.

En protégeant, de manière plutôt radicale il est vrai, ses secrets, la Chine a conservé pendant 3 millénaires le monopole de la production de la soie (à l'exception du Japon qui l'a obtenu de la

manière que je viens de décrire deux siècles avant notre ère, mais ne l'a utilisé qu'à des fins domestiques).

► Exemple 2 : l'arquebuse japonaise

Si le premier exemple illustre les conséquences économiques, le deuxième illustre les conséquences politiques de la propagation d'un savoir-faire. Il illustre en même temps, une méthode souvent utilisée dans l'histoire pour s'approprier les secrets. En 1543 le Japon ne connaissait pas les armes à feu et cinquante ans plus tard il était le pays du monde où elles étaient le plus utilisées. En 1575, les arquebuses ont joué un rôle clef dans la bataille de Nagashino et dans l'unification du Japon.

L'arquebuse a été transmise aux Japonais par des Portugais échoués sur les côtes de l'île Tanegashima. Si, tous les historiens s'accordent sur ce point, les arquebuses n'ont pas été volées aux marins portugais (elles ont été achetées par le seigneur local ou offertes par le capitaine du bateau échoué), le laps de temps très faible (6 mois) qu'il a fallu aux Japonais pour maîtriser la fabrication d'une arquebuse japonaise similaire au modèle portugais montre que les secrets de la technique leur ont été fournis. La légende dit qu'ils ont été obtenus par la demoiselle Wasaka, que son père, Kinbei Yasaka, fabricant d'épées de l'île, aurait chargée de s'approprier ! Une stèle à sa mémoire se visiterait encore sur les lieux du transfert technologique.

principe Responsabilité », a repris le thème du mythe, évoqué plus haut, de Prométhée, pour décrire les risques que certains choix humains mal maîtrisés en matière de développement technologique font peser sur la planète tant sur le plan social que sur les plans économique ou environnemental. Ceci pose la question de la responsabilité des scientifiques en matière de d'utilisation des résultats de leurs recherches. Même si, et effectivement tout le monde s'accorde sur ce point, ils ne peuvent pas être tenus pour responsables de ce que leurs gouvernements font de leurs découvertes, ils sont porteurs d'une responsabilité pour ce qui concerne la divulgation de leurs résultats.

Et, parce que les décisions dans ce domaine ne sont pas faciles à prendre, il est de la responsabilité des chercheurs de s'en remettre à l'institution de tutelle qui a hébergé leur réflexion et fourni les conditions de cette réflexion. Prendre en compte la protection des résultats dans son travail de tous les jours n'est pas un exercice facile pour un chercheur. Il requiert beaucoup d'attention et de la confiance en soi. Beaucoup de chercheurs

pêchent par excès de modestie et ne pensent pas que leurs recherches puissent intéresser l'industrie. De même, les chercheurs se sentent souvent démunis face à (ce qu'ils pensent être) la complexité des procédures. Mais, des solutions existent et les services de valorisation et d'aide à la création d'entreprise se développent tant dans les universités que dans les organismes de recherche déjà bien équipés. Le rôle des universités et des organismes de recherche, dans ce domaine, est de définir une politique de transfert industriel, de même qu'ils ont la mission de définir une politique de coopération internationale concertée et cohérente avec la politique industrielle.

Le développement anarchique et mal maîtrisé de coopérations universitaires ou scientifiques internationales a été, et est toujours, à l'origine de certains transferts de technologies, qui se font au détriment des pays qui les ont développées. Et sur le terrain de l'innovation la compétition est de plus en plus rude, pour deux raisons. La première est que le transfert de la recherche vers l'industrie est de plus en plus rapide et que les industriels ont de

moins en moins de « projets sur étagère » en attente de développement. Les versions et générations de produits se succèdent avec une telle vitesse que la prochaine génération a rarement plus de deux ans d'avance. La deuxième raison est que le nombre de pays possédant un potentiel d'innovation créative est de plus en plus grand. En effet, les pays de développement plus ancien ont très longtemps gardé le leadership, mais sont maintenant mis en concurrence par les pays qui accèdent plus tardivement au développement. Cette mise en compétition nouvelle doit être un facteur d'entraînement des chercheurs et doit être comprise comme telle. La coopération internationale dans les domaines scientifiques et technologiques ne doit pas être confondue avec l'aide au développement et n'est pas du ressort des mêmes institutions. Il ne s'agit pas de pointer du doigt certains pays ou de se fermer à toute coopération. Il s'agit de faire coïncider les intérêts nationaux avec les intérêts personnels et de faire coïncider les intérêts à moyen et à long terme avec les intérêts à court terme. ■

Le mal des mails

Par Joseph Illand

Fonctionnaire de sécurité de défense du CNRS
joseph.illand@cnrs-dir.fr

On connaît le mal des spams, mais a-t-on bien mesuré tous les dangers des transmissions par mails.

L'un peut se présenter « à découvert », comme dans un mail de menaces de mort reçu par une directrice de recherche « ...My work... is just to kill you and I have to do it as I have already been paid for that... ». Il peut être plus insidieux quand il incite, souvent très habilement, à « cliquer » sur un lien ou une pièce jointe. Et le clic va bien sûr provoquer l'installation d'un cheval de Troie ou d'un keylogger sur votre poste. Et comme on a beaucoup d'amis, et si la pièce jointe est drôle, on s'empressera de faire suivre le mail à tout son carnet d'adresse, en toute inconscience.

Le mail dont vous êtes l'auteur peut lui-même avoir des effets pervers.

Sauf à être chiffré, il est à la portée de tous les yeux curieux, il n'offre aucune garantie de confidentialité ni de discrétion :

- il peut être lu par un tiers qui n'est pas destinataire ;
- il peut être renvoyé par l'un ou l'autre des destinataires à des personnes dont vous ne souhaitez pas qu'elles aient connaissance de votre message (c'est déjà bien si vous êtes informé de cette retransmission !) ;
- il peut aussi être tronqué, modifié et garder l'apparence de votre paternité ;
- il peut se retrouver sur Internet en deux coups de cuiller à pot, retransmis sur des sites ou cité dans des forums.

Bien sûr ça n'arrive qu'aux autres ! Alors voyons quelques exemples d'aventures vécues récemment :

Un directeur d'une entité du CNRS traite une affaire délicate et sensible de délinquance interne (oui ! ça arrive au CNRS, comme partout ailleurs !). Il éprouve le besoin de faire un point sur l'affaire et de l'adresser par mail à un de ses interlocuteurs internes « Je t'envoie ce mail strictement confidentiel à ton adresse personnelle pour éviter toute fuite... », s'ensuit des impressions assez personnelles sur l'affaire... Dans les 3 minutes qui suivent, le mail fait déjà l'objet d'une rediffusion ! Un an plus tard, en appui d'une attaque contre le CNRS, le mail est transmis par

un correspondant anonyme à des personnalités régionales, à la direction du CNRS, au ministre de la Recherche... Il avait dit « confidentiel » ?

Dans un pays sensible où les intérêts de la France sont importants mais sujets à remise en cause (vous avez deviné qu'il s'agit de la Syldavie (*)), un agent du CNRS, affecté au Centre de Recherches Archéologiques de Klow, transmet à une bonne part de son carnet d'adresses (une soixantaine de destinataires) un texte « coup de gueule ». Traumaté par des travaux de fouilles archéologiques qui conduisent à la destruction des quartiers populaires de la zone orientale de Klow, l'agent s'en prend en termes passionnés à la « dictature » du régime Syldave, à la corruption de ses dignitaires ...et incite à poser une bombe. Envoyé à un cercle de parents et d'amis, le mail se retrouve quelques minutes plus tard en ligne sur

internet, grâce aux soins d'une amie très zélée. Qui plus est, alors que le texte ne comporte pas en clair la signature de l'auteur, l'amie intentionnée a rajouté dans son envoi pour mise en ligne, le nom, le prénom, et la fonction explicite de la personne. On passera sur les suites extrêmement douloureuses de cette affaire qui s'est passée en 2007, dans un pays bien réel et qui a failli être lourde de conséquences pour la coopération entre la France et ce pays.

Nul n'est à l'abri des imprudences, il est arrivé à l'auteur de ces lignes d'émettre une « mise en garde » à l'encontre d'une association active contre des travaux menés par le CNRS. Cette mise en garde s'est retrouvée quelques jours plus tard ... en ligne sur internet.

Plus grave : on se souvient de la mise en ligne en 2004, sur des sites universitaires, puis sur un site américain, d'un document

« confidentiel défense » de mise en garde émanant d'un Haut Fonctionnaire de Défense d'un ministère.

L'apposition d'un coup de tampon « confidentiel » ou la mention dans un mail de la phrase si souvent rencontrée pour des transmissions sensibles « attention, ce mail est hyper confidentiel, merci à celui qui n'est pas concerné de ne pas le lire », ne suffisent pas à éloigner les curieux.

En 2005, des échanges préparatoires à un dépôt de brevet effectués par mail avec ce genre de mention « protectrice » ont conduit à une publication étrangère sur le sujet, le jour même du dépôt de brevet.

La confidentialité ne s'obtient pas avec des incantations (surtout publiques), elle se garantit par des dispositions adaptées au degré de sensibilité de l'information. ■

(*) <http://fr.wikipedia.org/wiki/Syldavie>

PROTECTION DU PATRIMOINE SCIENTIFIQUE D'UNE UNITÉ DE RECHERCHE

A qui profite le crime ?

Par Jean-Luc Toffart

Adjoint au FSD pour la protection du patrimoine scientifique
jean-luc.toffart@cncrs-dir.fr

Il ne s'agit pas dans cet article de présenter un bilan exhaustif des problèmes réellement survenus dans certaines unités, mais de montrer au regard de quelques-uns d'entre eux comment des atteintes au patrimoine scientifique peuvent se manifester.

► Événements anodins ?

Un directeur adjoint, victime d'un vol à la portière sur son trajet travail domicile, se voit voler son ordinateur portable. Ce phénomène étant fréquent, et considérant que des sauvegardes sont régulièrement faites, il estime le préjudice réduit à la seule perte matérielle. Quelque temps après, survient un cambriolage au laboratoire même, et l'ordinateur portable du second directeur adjoint disparaît. L'événement est de nouveau perçu comme banal, bien que certains s'interrogent sur le fait que ce portable, situé dans un bureau éloigné de la sortie, ait été choisi à la place d'autres plus facilement accessibles. En revanche, personne ne s'inquiète

de l'intérêt des informations contenues dans cet ordinateur.

Un peu plus tard, c'est le directeur du laboratoire, lors d'un congrès à l'étranger, qui se fait dérober son ordinateur portable en pleine rue pendant son retour à l'hôtel. La perte a pu être mesurée directement cette fois, avec six mois de résultats de recherches perdus car d'importantes données scientifiques résidaient sur cet ordinateur sans qu'il n'y ait eu de sauvegarde. Après discussion avec les services spécialisés, le directeur a admis que l'accumulation des événements subis par son laboratoire pouvait ne pas être attribuée au seul hasard.

Cet ensemble de faits montre l'intérêt du signalement auprès du service du Fonc-

tionnaire de Sécurité de Défense de tout événement anormal de la vie du laboratoire. Une centralisation de l'information peut permettre d'identifier des liens dans une accumulation d'événements apparemment distincts et ne concernant d'ailleurs pas toujours le même laboratoire.

► Conséquences en cascade

Un laboratoire a subi pendant plusieurs mois des cambriolages d'origine crapuleuse. La mise en place d'une vidéosurveillance a permis d'identifier l'auteur mais la dernière de ses « visites » s'est soldée par un incendie important mettant hors service le serveur informatique. Pour assurer la continuité du service, un serveur du campus a été utilisé. Malheureusement, la configuration de celui-

ci n'était pas aussi sécurisée que celle du serveur défaillant. La conséquence a été quasi immédiate : dix-huit micro-ordinateurs de l'unité ont été piratés.

Une multiplicité d'événements, même si elle est parfaitement identifiée peut entraîner des conséquences imprévues en cascade et ce d'autant plus que la maîtrise de ces événements peut échapper totalement aux différents intervenants. Ceci montre la nécessité de définir une procédure de réaction engageant l'ensemble du système d'alerte d'une unité (directeur d'unité, délégation régionale, co-tutelle, service du fonctionnaire de sécurité de défense, éventuellement services de police) pour avoir le maximum d'efficacité lorsque l'évènement survient.

► Intérêts personnels

Un chercheur travaille en collaboration avec une société étrangère et se fait rétribuer par celle-ci. Cette société dépose dans son pays des brevets, avec le chercheur pour inventeur et sur les mêmes technologies que celles développées au laboratoire de rattachement du chercheur. Cette affaire a été découverte lorsque la société étrangère a voulu vendre son portefeuille de brevets.

Il faut se rappeler qu'un fonctionnaire ne peut percevoir une rémunération extérieure sauf pour des activités bien précises comme des charges d'enseignements, des prestations de consultance ou lors de la création de start-up.

Par ailleurs, dès qu'il participe à l'élaboration d'une invention, il doit en informer son employeur. Il sera cité comme inventeur sur la demande de brevet correspondante qui sera éventuellement déposée par son employeur.

► Questionnaire insidieux

Un chercheur lance une enquête comportant des données ethniques au sein du personnel d'un organisme avec des questions suffisamment précises pour permettre d'identifier les personnes interrogées. La base de données constituée n'est pas déclarée à la CNIL. Après rappel de la réglementation au chercheur, un dossier a été présenté à la CNIL, mais les observations et réserves de la commission ont finalement conduit à l'abandon de l'étude. La méconnaissance de la réglementation et la non anticipation des risques inhérents à l'enquête montre que toute recherche doit impérativement prendre en compte les contraintes légales du contexte de l'étude.

► Détournement de brevets

Un étudiant étranger interrompt sa thèse pour retourner dans son pays et y déposer avec un enseignant de son université d'origine un brevet sur les recherches effectuées dans le laboratoire français. Le laboratoire ne peut plus déposer le brevet. Bien que l'étudiant ait signé un accord de confidentialité, le contentieux avec l'université correspondante reste à ce jour non réglé.

► Imprudence

Les exemples précédents ne doivent pas faire oublier les imprudences qui sont le fait de chacun d'entre nous. Pour lire son courrier électronique, un chercheur en déplacement à l'étranger peut être amené à se connecter à partir d'un ordinateur local (celui de l'hôtel de résidence ou du lieu où se tient la conférence,...) ou même connecter son propre ordinateur sur un réseau local. Dans quelle mesure peut-il être certain que l'ordinateur à partir duquel il se connecte ou le réseau qu'il utilise ne récupère pas les identifiants et mots de passe de connexion ?

De même, quelques chercheurs ont eu la désagréable surprise dans certains pays, en débarquant de l'avion, de voir leur ordinateur portable « emprunté » lors d'un contrôle de sécurité. Le système est imparfait, l'ordinateur est perdu de vue pendant dix minutes. C'est amplement suffisant pour copier toutes les données figurant sur celui-ci. Il est donc important de s'assurer qu'aucune donnée sensible n'est présente sur l'ordinateur.

Les dommages au patrimoine scientifique revêtent donc des formes très variées, mais la plupart du temps ils sont facilités par négligence, volontaire ou non, et souvent aggravés du fait du manque d'anticipation des conséquences. Il s'y ajoute le fait de la méconnaissance de la réglementation ou même de son non-respect. L'importance des dommages est souvent minimisée.

Des données dérobées peuvent-elles justifier le vol des ordinateurs ? Probablement, mais les chercheurs ont du mal à le croire bien que leurs recherches puissent avoir de forts impacts économiques et donc susciter des convoitises. Cette « naïveté » est une chance pour un concurrent indelicat, un espion ou toute autre personne malveillante.

► Conclusions

La réputation d'un laboratoire, la valorisation de sa recherche, le portefeuille de ses contrats de recherche, la compétence de ses chercheurs et son potentiel technique sont des composantes essentielles de son « patrimoine scientifique ».

Il est donc important d'apporter une vigilance essentielle à la protection de ce patrimoine.

Les exemples cités montrent bien que cette protection est l'affaire de tous. Un dispositif est à définir et à mettre en place dans chaque unité. Celui-ci implique :

- la prise de conscience par chacun des enjeux, des menaces et de la vulnérabilité concernant le patrimoine à protéger ;
- l'accompagnement dans cette démarche du fonctionnaire de sécurité de défense avec un rôle d'aide et de conseil pour toutes ces tâches qui ne sont pas familières à tous ;
- la connaissance des relais hiérarchiques et fonctionnels (directeurs d'unité, délégations régionales, réseau des responsables de la sécurité des systèmes d'information) ;
- la possibilité de s'appuyer éventuellement sur des intervenants extérieur (audits, services du ministère de l'intérieur, ...).

Souvent une atteinte au patrimoine passe sur le moment inaperçue ou sa gravité est négligée. Les conséquences et les préjudices peuvent n'être constatés que beaucoup plus tard.

La connaissance des vulnérabilités d'une unité de recherche permet d'adapter les mesures de protection à prendre contre les menaces. ■

SÉCURITÉ DE L'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 4 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :

Joseph Illand
Fonctionnaire de Sécurité de Défense
Centre national de la recherche scientifique
3, rue Michel-Ange, 75794 Paris-XVI
Tél. : 01 44 96 41 88
Courriel : joseph.illand@cnrs-dir.fr
<http://www.sg.cnrs.fr/fsd>

Rédacteur en chef :

Robert Longeon
Chargé de mission SSI du CNRS
Courriel : robert.longeon@cnrs-dir.fr

Impression : Bialec, Nancy (France) - D.L. n° 69311

ISSN 1257-8819
Commission paritaire N°1010 B 07548
La reproduction totale ou partielle des articles est autorisée sous réserve de mention d'origine.