PAR PHILIPPE WOLF (78)

Trois théorèmes pour caractériser le cyberespace

sous-directeur « Télécommunications et Réseaux Sécurisés» au sein du SGDN, il enseigne l'intelligence économique au sein du département d'enseignement et de recherche en humanités et sciences sociales de l'École polytechnique

À la fois monde nouveau et reflet du monde réel, le cyberespace constitue un champ privilégié pour l'exercice de l'intelligence économique. Comprendre cette infosphère est un préalable à la définition et mise en œuvre d'une vraie stratégie en la matière. Cette appréhension peut s'articuler autour de grands principes structurants qui ont une force comparable à celles des théorèmes en mathématiques.

Le cyberespace, espace virtuel contenant des sociétés artificielles, peut se définir comme un espace social d'interaction entre une technologie – la numérisation de l'information et les processus de communications de celle-ci – et un ensemble d'êtres humains interagissant avec ces techniques. Il est la marque la plus éclatante de la globalisation de l'économie mais aussi le miroir parfois déformant des instabilités d'un monde secoué de convulsions permanentes. Les systèmes et réseaux informatiques sont devenus des outils indispensables pour les tâches critiques de la vie professionnelle et parfois même de la vie privée.

L'intelligence économique – pour certains la forme légale de l'intelligence, dans son acception anglo-saxonne de renseignement ou d'espionnage – a trouvé, dans cette infosphère, un champ d'action nouveau à la fois dans sa dimension temporelle d'immédiateté, dans sa dimension spatiale qui embrasse le monde et dans sa dimension cognitive qui fait renaître l'esprit encyclopédique.

L'arme du renseignement numérique stratégique

Le renseignement qu'il soit étatique ou privé, qui joue des ambiguïtés et des faiblesses d'un droit international numérique largement à construire, a résolument investi le cybermonde. Au-delà des légitimes motivations de sécurité nationale, le renseignement numérique stratégique est devenu une arme de la « guerre économique » qui provoque d'abord de la distorsion de concurrence quand il n'est pas parfois le moteur principal d'un développement industriel fondé sur la contrefaçon.

L'intelligence économique numérique (IEN) procède en premier de l'ensemble des technologies informatiques automatisant aussi loin que possible la pyramide classique du renseignement qui va de la donnée brute à la synthèse intelligente. La maîtrise de ces technologies est un facteur essentiel de compétitivité. L'innovation dans les techniques de fouille informationnelle ou « data mining » est très active et féconde. Au-

La cryptographie

La cryptographie est la seule technique disponible pour protéger l'information en confidentialité et en intégrité. Elle réalise une réduction d'entropie sur les données à protéger grâce à de multiples clés (une clé = un usage) qu'il s'agit de gérer comme les seuls secrets du système d'information. La gestion de ces clés est un art difficile qui nécessite une organisation rigoureuse qui se satisfait mal d'une externalisation trop poussée ou d'un recours à des solutions toutes faites.

La cryptographie n'est pas la solution miracle décrite par certains car elle doit s'accompagner d'une véritable politique de sécurisation en profondeur des systèmes d'information.

Ainsi, pour souligner les difficultés de toute nature s'opposant à une utilisation maîtrisée de cette technique, l'usage de la signature électronique dite « qualifiée », huit ans après la directive communautaire, reste marginale en France.

La cryptographie reste cependant au cœur des problèmes de gouvernance d'Internet. La création d'autorités européennes de certification pour l'ensemble des logiciels de communication (messagerie, navigateur...) commercialisés en Europe – une des mesures préconisées par la Commission européenne pour la libération de la croissance française – est toujours différée.

delà des outils, l'intelligence humaine et ses failles y occupent, bien sûr, une place centrale. Mais cet essor numérique s'est accompagné d'un développement des menaces liées à de nouvelles formes de criminalité allant des actions quotidiennes du cybervandalisme ou du cybercrime aux modes d'actions cachées de la cyberguerre ou du cyberterrorisme – s'il existe ailleurs que dans les romans ou dans les films – bien plus difficiles à caractériser ou à reconnaître. La dimension duale du recueil de renseignements consiste aussi à faire face à ces nouveaux risques.

Les caractéristiques du cyberespace

Il convient avant d'aborder, dans l'article suivant, le recueil et le traitement de l'information numérique et la protection de ses propres systèmes d'information, de mieux comprendre la nature profonde du monde numérique et des technologies qui l'animent. Car, sans capacité de protéger son propre patrimoine informationnel, aucune action d'intelligence économique numérique ne peut être vraiment efficace.
Trois « théorèmes » peuvent caractériser le cybermonde.

Théorème 1 :
toute information n'est pas bonne à numériser
Un fichier numérique se clone parfaitement. Il s'agit là d'une tautologie mais certains comportements numériques feignent de l'ignorer, même quand cela touche à l'intimité ou à l'affectif. Une information, dès sa numérisation achevée, peut être dupliquée à l'infini. Sa publication sur Internet lui procure instantanément une diffusion globale et une rémanence qu'il est impossible de mesurer. Cela ne signifie pas que l'information est éternelle et une bonne politique d'IEN se préoccupe aussi, au-delà des problèmes de formats numériques retenus, des formats physiques de stockage de ces données numériques et du problème de l'entretien de ces stocks numériques sur des supports qui subissent des dégradations et des altérations. Signalons d'ailleurs que la normalisation des formats numériques est aujourd'hui l'objet d'une bataille frontale entre les tenants des formats libres et ceux des formats propriétaires. Elle prolonge les débats houleux autour des brevetages logiciels. Ce clonage favorise les fuites d'information organisées ou accidentelles qui prennent parfois un retentissement que ne compense que la volatilité extrême des points d'intérêt. Toutes les manipulations sont possibles sur les réseaux numériques ouverts. Le faux y côtoie le vrai sans que le recoupement des sources ne permette, comme dans le renseignement traditionnel, une véritable qualification de la fiabilité de l'information. Enfin les rumeurs, les « traficotages de listings » et autres canulars peuplent le cybermonde avec des conséquences parfois démesurées comme des manipulations de cours en Bourse ou des déstabilisations de cadres d'entreprise.
Notons d'ailleurs que l'underground de l'Internet (siège des échanges interpersonnels) recèle une masse d'informations non visibles directement sur les navigateurs usuels mais accessibles par des outils largement diffusés. Au-delà des échanges de fichiers sous droits d'auteur (musiques et films), ces logiciels permettent la diffusion d'un savoir-faire autrefois couvert par le secret. On trouve par exemple sur Internet, pour qui sait fouiller, des recettes d'explosifs et des boîtes à outils permettant de construire des pièges informatiques. On peut y acheter également, par des ventes en ligne qui se jouent des frontières et parfois des lois locales, toute la panoplie des

Toutes les manipulations sont possibles sur les réseaux numériques ouverts

L'avance américaine

La politique « d'information dominance », prônée par les États-Unis depuis les travaux fondateurs des années 1990, s'accomplit réellement dans la maîtrise technologique des pièces logicielles et matérielles constituant les systèmes numériques d'aujourd'hui mais également par la mise en place d'une hypersurveillance dont l'emblème est le réseau Echelon. Ce terme désigne le système mondial d'interception des communications privées et publiques, élaboré par les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande dans le cadre du traité UKUSA « UKUSA Agreement ». Depuis l'activation en janvier 1993 du « National Industry Security Program » qui organise avec le Département de la Défense et une vingtaine d'agences gouvernementales la protection des entreprises, des universités et des centres de recherche américains, ces moyens ont été orientés également vers l'intelligence économique. Bill Clinton confirma explicitement en 1994 le rôle du renseignement en la matière. Concrètement, c'est « l'Office of Executive Support » au sein du Département du Commerce qui assume le lien entre les négociateurs du monde économique et les agences de renseignements. Des rapports européens discutent sans fin sur l'impact réel de ce système dont le fonctionnement relève du secret de défense. Echelon reste l'archétype des systèmes d'intelligence numérique stratégique dont sont dotées diverses agences de renseignements.

matériels d'espionnage (ou de contrôle domestique, comme cela est présenté pudiquement outre-Atlantique) que la miniaturisation de l'électronique et la sophistication des technologies sans fil rendent difficilement détectables.

Théorème 2 dit de la confiance : pour pouvoir parler d'informatique de confiance, il faut en maîtriser les techniques

Dans un article célèbre publié en 1984 *(Reflections on Trusting Trust)*, Ken Thompson, pionnier des systèmes d'exploitation et des logiciels de programmation modernes, piège nativement le « login » (fonction d'identification d'un système d'exploitation) en créant une porte dérobée quasiment indétectable *. Sa démonstration fait encore régulièrement l'objet de débats passionnés, mais traduit une réalité indéniable.

Au-delà du souhait de disposer de produits de sécurité pour essayer de contrer ces dispositifs, il sera également primordial de bien apprécier, par un travail de veille active, les travaux futurs allant vers l'Internet des objets (développements autour de l'Internet chinois, etc.). Dans ces délicats problèmes de confiance, un exemple plus insidieux est celui de certains produits du marché qui savent séduire les décideurs par leur ergonomie certes pratique, mais qui en font des cibles de choix pour l'intelligence économique. Enfin, des développements matériels déjà réalisés autour de coprocesseurs de sécurité, qui équipent les machines informatiques, font peser une lourde hypothèque sur les capacités futures de maîtrise partagée du cybermonde.

La puce Fritz

« Trusted Platform Module » (TPM) désigne les spécifications détaillées et publiques d'un cryptoprocesseur sécurisé appelé souvent « puce Fritz » du nom de Fritz Hollings, sénateur de la Caroline du Sud, qui travaille d'arrache-pied au congrès des États-Unis pour rendre ce composant obligatoire dans toute l'électronique grand public.

À l'image d'une carte à puce, ce circuit sert à enfuir des clés cryptographiques dans les matériels informatiques en les marquant individuellement.

À partir de ce coffre à clés peuvent être développées tout un ensemble de fonctions de sécurité comme la gestion des droits numériques – les fameuses DRM si décriées –, et d'autres plus complexes comme l'isolation mémoire, la protection interapplications, les entrées-sorties sécurisées, le stockage scellé ou l'attestation à distance.

Ces fonctions permettront, peut-être, de lutter contre la piraterie informatique mais verrouilleront, à coup sûr, un usage libre de l'informatique.

La maîtrise de ces techniques sera un enjeu essentiel des « guerres de l'information » futures. Il est à craindre que les concentrations industrielles sur les marchés du *software* et du *hardware* qui se font majoritairement en dehors de l'Europe ne nous laissent dans une situation de réelle défiance vis-à-vis de ces développements.

La sécurité par l'obscurité

Les filtres anti-tout commercialisés par le marché de la sécurité informatique (antivirus, antispyware, antiphishing, anti-rootkits, antispam, etc.) pas plus que la cryptographie ne sont les solutions miracle annoncées. Ils participent de la « sécurité par l'obscurité » qui n'a jamais démontré ses vertus dans la lutte effective contre la criminalité informatique dont le maître mot est : « pas vu, pas pris ». Le premier virus de l'histoire (ver Morris de 1988) a paralysé l'embryon d'Internet en s'attaquant à une faille du service de messagerie. Le courriel reste aujourd'hui le vecteur privilégié des attaques informatiques.

Théorème 3 dit « théorème du virus » : la détection d'un virus est indécidable à la fois par une analyse* a priori *ou par une analyse dynamique

Ce théorème, exposé en 1984 par Fred Cohen qui a réalisé la première étude *in vivo* sur les virus informatiques au sein de la « National Security Agency », est une variante logique du théorème de Rice qui démontre, en théorie de la calculabilité, que le problème de l'arrêt d'un programme informatique quelconque n'est pas décidable. Au-delà de l'aspect mathématique, il manifeste une double réalité : les pièges informatiques nouveaux contournent régulièrement les barrières installées et la fortune des vendeurs d'antivirus est assurée pour toujours.

Quand les enjeux de sécurité sont importants, seule une isolation physique d'un système d'information permet d'assurer une vraie protection, le risque zéro existant ici moins qu'ailleurs. Pour citer un exemple, la France s'est ainsi dotée d'un intranet sécurisé interministériel pour la synergie gouvernementale (ISIS) qui est le premier système d'information sécurisé national permettant l'échange et le partage de documents classifiés au titre du secret de défense entre acteurs gouvernementaux. Outil de travail quotidien pour le traitement des informations classifiées, c'est aussi un outil de conduite de l'action gouvernementale lors d'une situation d'urgence ou d'une crise. ■

Seule une isolation physique permet d'assurer une vraie protection

* *The moral is obvious. You can't trust code that you did not totally create yourself (especially code from companies that employ people like me).*