PAR PHILIPPE WOLF (78)

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

Une dimension nouvelle dans le **monde virtuel**

Le cyberespace nous fait entrer dans une dimension nouvelle des activités humaines. Un outillage de plus en plus sophistiqué permet un développement sans précédent de la collecte et de l'analyse des données disponibles, permettant la constitution d'un authentique patrimoine informationnel. Patrimoine qu'il est impératif de protéger par la mise en œuvre d'une politique de sécurité en constante évolution, politique qui relève avant tout de l'intelligence humaine.

Pour une entreprise ou une organisation, l'intelligence économique numérique (IEN) doit procéder de deux pratiques complémentaires et inséparables.
Tout d'abord la constitution, l'entretien et l'usage d'une base informationnelle irriguant l'ensemble de son savoir-faire : le développement de cette base fait appel à des outils informatiques en permanente évolution.
Ensuite la protection de son propre système d'information combinée à la maîtrise de sa communication numérique.

Un véritable arsenal d'armes logicielles

L'enregistrement et la diffusion de données de plus en plus nombreuses et variées ont permis de construire des outils de fouille informationnelle (« data mining ») dont la sophistication devient surprenante.
De nouvelles techniques d'analyse de la parole, de traduction multilangue automatique ou de modélisation des processus cognitifs sans parler de la révolution de l'imagerie numérique enrichissent la trousse à outils de cette révolution du renseignement numérique qui touche directement quatre des six domaines édictés par la Direction générale du renseignement extérieur (DGSE) à savoir : le renseignement d'origine électromagnétique (ROEM), le renseignement d'origine image (ROIM), le renseignement d'origine opérationnelle (ROOPS) et, bien sûr, le renseignement de source ouverte (Info SO). Dans le domaine du renseignement d'origine humaine (ROHUM) on peut également prévoir une intrusion croissante du numérique marquée, par exemple, par les addictions technologiques de l'homme moderne ou l'explosion des réseaux sociaux virtuels.

REPÈRES

On ne peut s'empêcher de penser à l'adaptation cinématographique de la nouvelle éponyme de Philip K. Dick, *Minority Report*, dont le cadre est le Washington de 2054 où des êtres humains mutants, les Précogs, peuvent prédire les crimes à venir grâce à leur don de prescience dans l'organisation appelée « Precrime ».

La vitalité et la variété extraordinaire de ces recherches algorithmiques commencent également à irriguer l'intelligence économique. Une technique essentielle est ici la fusion d'informations qui correspond à la volonté d'utiliser simultanément plusieurs sources de données, ou de grouper des informations hétérogènes afin d'obtenir une nouvelle information de meilleure qualité pour une meilleure décision. Il s'agit souvent à partir de signaux faibles et d'une observation imparfaite de la situation de former des hypothèses partielles.
La gestion des crises (catastrophe naturelle, attaque terroriste, crise sanitaire, crise systémique...) aussi bien dans leur anticipation (prévention et alerte) que dans leur traitement bénéficie de ces technologies qui permettent de mieux comprendre et de partager une vision commune aux acteurs économiques pour mieux agir. Dans la gestion postcrise qui a pour objectif d'améliorer la résilience en restaurant l'activité, l'analyse des retours d'expérience permet également d'enrichir la base d'IEN. L'entretien d'un patrimoine informationnel dynamique peut également être porteur de « sérendipité » qui est le fait de comprendre que l'on a trouvé ou

découvert par hasard, par chance ou par accident, quelque chose d'important que l'on ne cherchait pas. On rejoint ici les techniques modernes de la guerre infocentrée. La création de « war rooms » numérisées au sein de certaines entreprises procède de ces nouveaux processus de management actif.
Dans ces technologies de pointe, des pôles de compétitivité en France, coordonnant les travaux de PME et de grandes entreprises, essaient de structurer l'innovation autour de thématiques en partie sécuritaires. Deux exemples peuvent être cités. Infom@gic, qui relève de l'ingénierie des connaissances, en explore trois axes technologiques fondamentaux : les moteurs de recherche avancés, l'extraction de connaissances et la fusion d'informations multimédias, et ce sur tous les types de sources. System@tic, dans sa thématique sécurité et défense en particulier, traite des innovations significatives en matière de technologies logicielles et d'architecture de grands systèmes complexes.

Neuf principes pour bâtir une politique de protection de ce patrimoine

L'autre dimension de l'IEN consiste pour une entreprise, une administration ou un pays à savoir sécuriser ses systèmes et réseaux d'information selon les pratiques d'une science désignée, en France, sous le sigle SSI (Sécurité des systèmes d'information).
Au-delà des problèmes classiques de vol ou de piégeage de matériel comme les portables ou les supports amovibles, et du traitement systématique des traces électroniques, des formes nouvelles de menace sont apparues ou se sont développées. Des événements récents démontrent clairement que les mafias, les officines privées d'intelligence économique et les services de renseignements étrangers savent profiter des vulnérabilités non traitées des nouvelles technologies.
L'OCDE a établi neuf principes qui permettent un examen rapide des défis à relever pour l'IEN et la SSI (Sécurité des systèmes d'information) dans leur dimension défensive. L'OCDE plaide, bien évidemment, pour un point de vue global et cohérent. Ces recommandations n'ont pas un caractère obligatoire.
1 – Sensibilisation. Le référentiel des formations en intelligence économique, élaboré dans le cadre de la mission du haut responsable en charge de l'intelligence économique, liste, dans ses quatre grands thèmes d'enseignement, l'économie de l'information et de la connaissance. Plus largement, des actions de sensibilisation doivent être régulièrement organisées au sein des entreprises ou des organismes pour faire prendre conscience des risques numériques et des enjeux des bonnes pratiques dans l'espace numérisé. Une place doit y être consacrée dans les cursus scolaires à tous niveaux et cela passe obligatoirement par une formation des formateurs.
2 – Responsabilité. « Chaque acteur des systèmes d'information a une part de responsabilité dans la SSI. » Il s'agit aussi, concernant la base IEN, de bien définir le besoin d'en connaître et de fixer les apports de chacun à un travail de veille qui ne peut être que collectif.
3 – Réaction. « Ce principe évoque l'utilité d'agir de manière réactive et coopérative pour prévenir, détecter et répondre aux incidents. » Une pratique régulière d'exercices à partir de scénarios simples a démontré sa pertinence. ➤

Une création orwellienne

Quelques semaines après les attaques du 11 septembre 2001, l'amiral John Poindexter – connu pour avoir été mêlé au scandale de l'Irangate – propose comme responsable du « Information Awareness Office », un des principaux programmes de renseignement du DARPA (Département de la recherche de défense aux USA) de réaliser un système d'information intitulé « Total Information Awareness System » (TIA).
Il s'agit de développer un système modulaire et automatique apte à révéler des activités prototerroristes.
TIA recueille, pour tout individu identifié dans le système par ses marquants biométriques – photographie faciale, empreintes digitales, iris, déambulation, etc. –, l'ensemble de ses traces numériques dans une liste à la Prévert qu'il n'est pas utile de traduire : Financial, Education, Travel, Medical, Veterinary, Country/Entry, Place/Event Entry, Transportation, Housing, Critical Resources, Government, Communications.
Toute une panoplie de logiciels d'analyse multi-agents, de recherches sémantiques de connexions, de modélisation comportementale et de reconnaissance de « patterns » caractéristiques fouille, en permanence, cette métabase de données dynamique pour avertir, *in fine*, des analystes humains sur un événement clé en moins d'une heure.
Après une bataille médiatique d'associations de protection des libertés civiles, le programme a été rebaptisé « Terrorist Information Awareness System ». Depuis, peu d'informations ont filtré sur l'avancée de TIA (il est éliminé du budget de la Darpa dans les dépenses militaires approuvées par le Sénat pour 2004) et, bien sûr, sur son efficacité réelle.

Certains prédisent une avancée dans la manipulation mentale

4 – Éthique. « Les parties prenantes doivent adopter une conduite éthique afin de ne pas causer de tort à autrui. Cela consiste notamment à adopter des pratiques exemplaires et promouvoir des comportements qui tiennent compte des impératifs de sécurité et respectent les intérêts légitimes des autres parties prenantes. » Cette recommandation s'oppose souvent à l'impunité qui règne dans le cyberespace.

5 – Démocratie. « La SSI doit être compatible avec les valeurs des sociétés démocratiques, notamment la liberté d'échanger des pensées et des idées, la libre circulation de l'information, la confidentialité de l'information et des communications, la protection adéquate des informations à caractère personnel, l'ouverture et la transparence. » Les 30 pays membres actuels de l'OCDE ont une pratique numérique globalement compatible avec les contradictions apparentes de cette recommandation (transparence *versus* protection).

6 – Évaluation des risques. « Évaluer les risques SSI, particulièrement en termes d'importance des informations à protéger, de menaces, de vulnérabilités et de préjudices possibles, permet de déterminer un niveau acceptable de risque et des mesures de sécurité appropriées. » Sans travail méthodologique systématique de type « gestion du risque », il est illusoire de prétendre protéger, dans toute sa complexité, son patrimoine informationnel numérique.

7 – Conception et mise en œuvre de la sécurité. « Ce principe rappelle qu'il est primordial de considérer la sécurité comme un élément essentiel des systèmes d'information. » En particulier, les contractualisations en matière de systèmes d'information et de communication doivent comporter des clauses touchant à la sécurité dont l'impact soit estimable.

8 – Gestion de la sécurité. « Il est nécessaire d'adopter une approche globale et continue de la gestion de la sécurité, basée sur l'évaluation des risques SSI. » La sécurité se gère au quotidien par l'analyse pertinente des traces informatiques, par l'application des mises à jour de sécurité, par l'appel régulier à des audits, par la mise en place d'indicateurs permettant de mesurer les progrès.

9 – Réévaluation. « Le dernier principe prévoit de réévaluer régulièrement la SSI et de mettre à jour les politiques, référentiels et mesures de sécurité afin de prendre en compte l'évolution naturelle des risques. »

L'application de l'ensemble de ces recommandations procède du concept raisonné de la « défense en profondeur » et non d'une solution « clé en main » car comme l'affirme le philosophe Clément Rosset dans *Le réel et son double* : « *La fausse sécurité est plus que l'alliée de l'illusion, elle en constitue la substance même.* »

La fausse sécurité constitue la substance même de l'illusion

Des logiciels malicieux

L'année 2007 a marqué une rupture dans la sophistication et l'ampleur des attaques sur Internet. On citera, entre autres, les cyberattaques ciblées dites chinoises (origine largement inconnue), la saturation des réseaux estoniens par des attaques en déni de service (première cyberguerre pour certains commentateurs), l'extension des réseaux de machines compromises (botnet Stormworm), etc. Vincent Cerf, parfois appelé le « père de l'Internet », a annoncé à la conférence de Davos, en 2007, qu'une machine sur quatre recelait au moins un logiciel malicieux ou « malware ».

Conclusion

Le cybermonde nous fait pénétrer dans une dimension nouvelle des activités humaines. L'intelligence économique numérique connaît un développement sans précédent en s'appuyant sur un outillage de plus en plus sophistiqué. Son exploitation, qui nécessite la mise en place d'une véritable politique de SSI, relève cependant d'abord de l'intelligence humaine. ■

BIBLIOGRAPHIE

- Edward WALTZ, *Information Warfare : Principles and Operations*, Artech House, 1998.
- James BAMFORD, *The Shadow Factory, The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*, Doubleday, 2008.
- Jean-Louis DESVIGNES, *Les enjeux de la sécurité des systèmes d'information*, http://www.sstic.org/SSTIC03/articles/SSTIC03-Desvignes-Les_enjeux_de_la_securite_des_SI.pdf
- Ken THOMPSON, *Reflections on Trusting Trust*, http://www.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf
- L'intranet sécurisé interministériel pour la synergie gouvernementale (ISIS) http://www.ssi.gouv.fr/isis/
- La défense en profondeur appliquée aux systèmes d'information, http://www.ssi.gouv.fr/fr/confiance/documents/methodes/mementodep-v1.1.pdf
- Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité, http://www.ssi.gouv.fr/fr/dcssi/OCDE-lignesdir.pdf
- Portail de la sécurité informatique : http://www.securite-informatique.gouv.fr/
- Total « Terrorism » Information Awareness, http://epic.org/privacy/profiling/tia/