La protection des infrastructures critiques de l'information relève-t-elle de l'État ou de l'économie?

Depuis les années nonante, de nombreux États modernes ont commencé à se préoccuper des questions relevant de la protection des infrastructures critiques de l'information (Pici ou CIIP en anglais) et à l'intégrer à leur politique de sécurité. Si cette protection est importante, c'est que non seulement l'économie et l'État, mais aussi la prospérité de tous les citoyens dépendent de plus en plus de la disponibilité permanente des «systèmes nerveux numériques». La privatisation, dès les années quatre-vingt, de nombreuses entreprises publiques vitales pose le problème crucial de savoir à qui incombe, de l'État ou du secteur privé, la responsabilité des mesures et de la prévention à adopter dans le cadre de la sécurité nationale, la situation et le domaine demandant encore à être précisé.

La société, l'économie et l'État dépendent toujours plus d'«infrastructures critiques de l'information». On estime que 25% des entreprises feraient faillite en cas de panne informatique générale, à moins que celle-ci ne soit réparée très rapidement
Photo: Photos.com

Une dépendance toujours plus grande envers les infrastructures de l'information

Suite au progrès rapide de la révolution informatique et du maillage croissant des sociétés modernes, la dépendance vis-à-vis de ce qu'on appelle les «infrastructures critiques», et notamment celles qui concernent l'information, ne cesse de croître. Les informations véhiculées par ces réseaux, de même que les prestations et les processus qu'elles permettent, constituent fréquemment la base sur laquelle s'appuie le fonctionnement de toutes les autres infrastructures, d'où leur intérêt particulier (voir *encadrés 1* et *2*).

Les États modernes tels que la Suisse ont beaucoup à perdre si leurs infrastructures de l'information étaient frappées par une panne majeure. Plus de 70% des personnes actives occupées en Suisse travaillent dans le secteur des services et, selon des estimations, 25% des entreprises feraient faillite en cas de panne informatique générale, à moins que celle-ci ne soit réparée très rapidement. Pour une banque, par exemple, ce serait déjà le cas après deux jours de panne, et tout au plus trois pour une entreprise commerciale.[1] Cette dépendance et les risques et dangers qui en découlent pour la société, l'économie et l'État sont de plus en plus reconnus par les décideurs et les responsables.

Isabelle Abele-Wigert
Équipe d'analyse du risque, Centre de recherches sur la politique de sécurité, EPF Zurich

1 Interview en ligne de Reto Stäheli, directeur des Business Continuity Services, Swisscom IT Services.

Encadré 1

Pic et Pici

La protection des infrastructures critiques (Pic ou CIP en anglais) n'est pas une notion nouvelle; les États s'en soucient depuis longtemps. Autrefois, on connaissait surtout la protection des ouvrages vitaux à la défense nationale. De nos jours, la dépendance croissante vis-à-vis des technologies de l'information et de la communication (Tic) a déplacé l'attention vers la protection des infrastructures critiques de l'information (Pici). Il s'agit d'en protéger les éléments matériels (ordinateurs ou câbles à fibres optiques, par exemple) et virtuels (systèmes interconnectés, flux de données ou Internet). La Pici a pour mission de rendre exceptionnelles les ruptures de réseau et de système; qu'elles soient de courte durée, maîtrisables, limitées localement, et ne causent que des dégâts de peu d'ampleur. En d'autres termes, il s'agit de consolider les prestations vitales pour le pays.

Encadré 2

Les infrastructures critiques en Suisse

En Suisse, les *infrastructures* suivantes sont considérées comme particulièrement vitales: gouvernement et administrations publiques, services d'urgence et de sauvetage, (télé)communications, approvisionnement énergétique, services financiers et assurances, industrie et artisanat, médias, transports et logistique, système de santé et approvisionnement en eau.

Les *infrastructures critiques de l'information* comprennent plus spécifiquement, d'après les experts de la Confédération, la téléphonie, la télécopie, l'accès à Internet par le réseau fixe, le réseau mobile, les satellites (GPS, etc.), les réseaux de communication des CFF et de l'industrie électrique, les médias électroniques, l'émetteur radio à ondes courtes Bern-Radio, enfin les réseaux radio des autorités et du Bors (organisation suisse alémanique des services de sauvetage et de sécurité).

Libéralisation et privatisations modifient la donne

Suite à la libéralisation et à la privatisation de nombreuses régies publiques (eau, électricité, transports ou téléphonie), une grande partie des infrastructures vitales (de l'information) se trouve en mains privées, même en Suisse. Cela pose la question cruciale de savoir à qui incombe, de l'État ou du secteur privé, la responsabilité des mesures et de la prévention à adopter dans le cadre de la sécurité nationale, la situation et le domaine demandant encore à être précisé.

En matière de Pici, les intérêts de l'économie et de l'État sont en principe les mêmes, puisque les conséquences d'une longue panne seraient catastrophiques pour l'un comme pour l'autre: il leur faut à tout prix assurer un fonctionnement sans problème et une disponibilité constante des infrastructures de l'information. Toutefois, comme les entreprises doivent toujours minimiser leurs coûts tout en maximisant leurs gains, elles ne sont pas toujours prêtes à engager les ressources suffisantes à la sécurité et à la gestion des crises, au-delà de la simple protection technique des informations.

Les différents aspects du problème

Il ne suffit pas de considérer la Pici comme un simple problème de sécurité informatique, que les seuls moyens techniques permettraient de résoudre (logiciels anti-virus, pare-feu, codage des données, respect de normes particulières, etc.). Pour que les mécanismes commerciaux essentiels fonctionnent en permanence, il est tout aussi important de *prendre en compte les facteurs organisationnels et humains*, et de promouvoir ce qu'on appelle les partenariats public/privé (PPP).

L'*aspect pénal* représente une autre dimension du problème: faute de procédures efficaces de poursuite pénale, de modifications de la législation nationale et de coopération internationale, la société et ses infrastructures critiques ne peuvent être protégées de la criminalité informatique.

Viennent enfin les questions qui dérivent de la *politique de sécurité*, donc les scénarios qui dépassent les petits problèmes quotidiens des exploitants privés d'infrastructures et qui prennent une ampleur nationale; que l'on songe par exemple aux pannes d'électricité aux États-Unis. Pour empêcher de tels événements ne se produisent, il est d'indispensable d'intervenir aux niveaux technique, organisationnel, législatif et international.

Les échanges d'information et la coopération sont essentiels

Ces différents aspects de la Pici peuvent poser des problèmes de compréhension et susciter des conflits d'intérêt lors de la recherche d'outils efficaces et de solutions communes. Il est primordial que les interlocuteurs privés et publics échangent leurs informations dans un esprit de coopération, et que celles-ci circulent au sein de chaque secteur.

Le secteur privé ne manifeste, pourtant, pas toujours d'intérêt à cette coopération, même s'il présente parfois des carences au niveau stratégique, par exemple dans le domaine de la lutte contre le terrorisme, qui pourraient être comblées par l'État. Il existe trois raisons essentielles à cela:

- on craint d'abord qu'une fois partagées avec l'État, des informations «sensibles» sur des problèmes avérés de sécurité ne soient pas traitées avec la précaution requise, ce qui pourrait entacher la réputation de l'entreprise;
- ensuite, de nombreuses entreprises établies en Suisse traitent l'essentiel de leurs affaires à l'étranger;
- enfin, l'économie considère la Pici dans une perspective d'entreprise: elle s'intéresse davantage à la continuité des affaires qu'à l'aspect politique de la sécurité.

L'État doit donc convaincre l'économie que la Pici a un aspect politique et que les entreprises devraient en tenir compte, dans leur propre intérêt, dans leur analyse des risques et leurs plans d'urgence.

Le modèle des quatre piliers de la Confédération

En Suisse, au niveau fédéral, une foule d'entités administratives s'occupent de la protection des infrastructures critiques de l'information.[2] Le cœur du système est depuis quelques années le modèle dit des quatre piliers, qui prend en compte les divers aspects de la Pici, et qui se compose des éléments et protagonistes suivants.

La prévention

La prévention consiste à veiller par des mesures techniques et organisationnelles, mais aussi humaines (formation, information), à ce qu'il se produise aussi peu d'incidents que possible. Elle s'effectue, entre autres, par une analyse sectorielle des risques menée par les exploitants des infrastructures vitales, dans le cadre de l'approvisionnement économique du pays. La *Centrale d'enregistrement et d'analyse pour la sûreté de l'information (en allemand «Melde- und Analysestelle Informa-*

2 Voir Wigert (2005).

Encadré 3

Risques et menaces

Les infrastructures critiques de l'information sont d'abord exposées à des cas de «force majeure» comme les catastrophes naturelles, les accidents «de civilisation» (rupture de barrage, explosion de centrale nucléaire, etc.) et les réductions de main-d'œuvre (grève ou épidémie). D'autres risques peuvent naître des défauts organisationnels d'origine technique ou humaine: erreurs humaines (actives ou passives), pannes techniques, dépendances, goulets d'approvisionnement, (cyber)terrorisme ou ce qu'on appelle «Information Operations»[a], pour ne citer que quelques exemples. L'État et les entreprises – quelle que soit leur taille – doivent aussi se protéger des dangers qui pèsent sur les infrastructures de l'information du fait de leurs propres collaborateurs et de ce qu'on appelle le «Social Engineering»[b].

a Opération consistant à attaquer les systèmes d'information de l'adversaire tout en protégeant les siens.

b Obtention d'informations confidentielles par une approche de type «contact social» des détenteurs de secrets.

Encadré 4

Bibliographie

- Dunn Myriam et Wigert Isabelle, *The International Critical Information Infrastructure Protection (CIIP) Handbook,* Zurich, Forschungsstelle für Sicherheitspolitik, 2004.
- Henriksen Stein, «The Shift of Responsibilities within Government and Society» et Andersson Jan Joel et Malm Andreas «Minding the Gap: Reconciling Responsibilities and Costs in the Provision of Societal Security» dans *CRN-Workshop Report. Societal Security and Crisis Management in the 21st Century*, Stockholm, 2004.
- Informatikstrategieorgan Bund ISB, *Verletzliche Informationsgesellschaft. Herausforderung Informationssicherheit*, Berne octobre 2002
- Joint Economic Committee, United States Congress, *Security in the Information Age. New Challenges, New Strategies, Washington*, mai 2002, p. 12. Internet: *www.fas.org/irp/congress/2002_rpt/jec-sec.pdf*.
- Metzger Jan, «The Concept of Critical Infrastructure Protection (CIP)», *Business and Security: Public-Private Sector Relationships in a New Security Environment* (sous la dir. d'A.J.K. Bailes et d'I. Frommelt), Oxford, 2004.
- The President's Commission on Critical Infrastructure Protection (PCCIP), *Critical Foundations: Protecting America's Infrastructures*, Washington, octobre 1997.
- The White House, *The National Strategy to Secure Cyberspace*, Washington, février 2003.
- Wigert Isabelle, «Der Schutz kritischer Informationsinfrastrukturen in der Schweiz: Eine Analyse von Akteuren und Herausforderungen», *Bulletin 2005 zur schweizerischen Sicherheitspolitik* (sous la dir. d'Andreas Wenger), Zurich, Forschungsstelle für Sicherheitspolitik, 2005.

tionssicherung», Melani), entrée en service l'an dernier, assume un rôle important au niveau fédéral sur ce plan là. Elle a pour tâche d'informer aussi bien la population et les PME que les exploitants d'infrastructures critiques du danger de recourir à des technologies risquées et dont la mise au point laisse à désirer, et de leur signaler les lacunes au plan de la sécurité. Melani est dirigée par l'Unité de stratégie informatique de la Confédération (Usic) et soutenue par le service d'analyse et de prévention de l'Office fédéral de la police (Fedpol) et le «Computer Emergency Response Team» (Cert) de la fondation Switch. Alors que l'Usic se concentre avant tout sur la prévention et que la Fedpol centralise les renseignements, le Cert fait office de centre de compétence et de support technique.

La détection précoce

Melani doit le plus possible détecter à temps les dangers et les situations menaçantes pour que les dispositifs de défense puissent être mis en place et les technologies à risque être évitées.

La gestion des crises

Avec le concours de l'Infrastructure de la technologie de l'information et de la communication (en anglais «Information and Communication Technology Infrastructure», ICT-I) de l'Office fédéral pour l'approvisionnement économique du pays (Ofae), l'état-major spécial Information Assurance (en allemand «Sonderstab Information Assurance», Sonia) est l'organe stratégique de gestion des crises qui veille à ce que les conséquences de pannes sur l'État, l'économie et la société soient réduites à leur minimum.

Résolution technique des problèmes

Les causes techniques des pannes doivent être élucidées, analysées et éliminées. Les premiers responsables sont ici Melani et les partenaires des services fédéraux et de l'économie.

Maintenir l'équilibre entre les standards de sécurité et la rentabilité économique

La Suisse ne dispose ni d'une stratégie nationale générale de protection des infrastructures vitales de l'information, ni d'une instance centrale qui s'occupe exclusivement de Pici. Par tradition, les compétences disponibles et les savoirs éprouvés sont exploités là où ils existent déjà, à savoir dans les départements et organes spécialisés. Étant donné l'ampleur du domaine auquel s'intéresse la Pici, certains de ses aspects sont confiés à différentes organisations, ce qui peut sembler logique, mais crée aussi des flous.

Il est loisible de constater qu'à quelques exceptions près, les infrastructures de l'information que l'État entend protéger au nom de la sécurité nationale sont aussi celles qui forment la base de la compétitivité et de la prospérité de la Suisse. Vu sous cet angle, il est logique qu'un des principaux acteurs stratégiques de la politique helvétique de la Pici, à savoir l'Usic, soit rattaché au Département fédéral des finances (DFF).

Il est aussi évident qu'en ce qui concerne les petits dangers «quotidiens» qui menacent les infrastructures de l'information (virus, piratage informatique ou brève interruption des systèmes), c'est aux exploitants (privés) d'infrastructures eux-mêmes qu'il incombe de veiller à ce que cette protection soit adéquate. Comme d'autres États, la Suisse met l'accent sur la responsabilité propre de chaque entreprise. L'État ne régule qu'en cas de nécessité et doit trouver un équilibre convenable entre les normes de sécurité et la rentabilité économique. En revanche, si les dangers qui menacent nos infrastructures de l'information entrent dans la catégorie des attentats terroristes ou proviennent d'autres États, on s'attend à ce que les pouvoirs publics interviennent, puisqu'il s'agit d'un problème de sécurité nationale.

Un partenariat entre l'État et l'économie privée

La protection de l'information est un processus dans lequel les échanges permanents d'expériences jouent un rôle crucial La mise sur pied systématique d'un système général d'information, de gestion des crises et de protection des infrastructures de l'information, telle qu'elle est prévue dans le modèle dit des quatre piliers, ne peut donc se faire que si l'État et l'économie collaborent étroitement. Le système suisse de milice est précieux de ce côté-là, car les échanges entre politique et économie relèvent d'une longue tradition. ▮