Cybersécurité

EN 1988, L'UTILISATION DE L'INTERNET PAR LE PUBLIC n'en était qu'à ses balbutiements et le Règlement des télécommunications internationales (RTI) élaboré cette année-là ne contenait pas de dispositions explicites sur la cybersécurité. Il indiquait toutefois, dans son Article 9, qu'il fallait éviter de causer un «préjudice technique», principe ajouté du fait de la propagation du «Ver de Morris», qui était à l'époque l'un des tous premiers programmes malveillants. La cybersécurité a pris une importance considérable au cours des décennies suivantes et sera donc prise en considération lors de la révision du RTI. Certaines propositions consistent à ajouter des articles au traité ou à modifier des articles existants pour y faire figurer des éléments liés à la sécurité, notamment des mesures de lutte contre le spam.

Les cyberattaques sont de plus en plus nombreuses et de plus en plus sophistiquées. Dans le même temps, nous dépendons de plus en plus de l'Internet et d'autres réseaux pour des services et des informations à caractère essentiel. Selon l'entreprise de sécurité McAfee, le nombre de menaces recensées a atteint un niveau record en 2011. Au moins 70 millions de programmes malveillants différents circuleraient dans le monde et les téléphones intelligents en sont devenus un des vecteurs de propagation. Selon les analystes, au moins 70% des courriers électroniques sont des spams.

Pendant ce temps, les réseaux électriques intelligents, l'informatique en nuage, les réseaux d'automatisation industrielle, les systèmes de transport intelligents, les systèmes de cybergouvernement et les services bancaires électroniques – pour ne citer que quelques-uns des nouveaux types d'infrastructure – sont de plus en plus interconnectés. Une défaillance de l'un peut avoir des répercussions sur les autres. Ainsi, une commodité et une efficacité accrues vont de pair avec une vulnérabilité aux cyberattaques[1] elle aussi accrue.

Pour autant, la cybersécurité n'a pas encore de définition acceptée à l'échelle mondiale, ce qui freine les mesures de protection, qui doivent être prises à la fois au niveau national et au niveau international, puisque les réseaux et les systèmes informatiques d'aujourd'hui ne connaissent pas de frontières.

En règle générale, les incidents relatifs aux technologies de l'information et de la communication (TIC) sont soumis au code pénal en vigueur au niveau national, lequel, bien souvent, n'est pas mis à jour ou ne suit pas la tendance internationale. Nous ne disposons pas de codification internationale commune des délits concernés: ces délits doivent-ils comprendre le piratage de logiciels, par exemple, et la diffusion de pornographie enfantine? La fraude financière ou encore les attaques par déni de service? La réponse pourrait consister à harmoniser les législations nationales et à instaurer un cadre juridique pour permettre la coopération internationale. D'aucuns considèrent cependant que ces mesures ne sont pas nécessaires ou ne devraient être prises qu'au niveau régional.

Légiférer n'est pas la seule solution, ni la plus rapide, face aux cyberattaques. Les solutions techniques peuvent être complétées par des normes en vue d'assurer l'interopérabilité et le respect des mesures de sécurité. Ce point est particulièrement important en raison de l'interdépendance des réseaux dans le monde d'aujourd'hui. Le Secteur de la normalisation des télécommunications de l'UIT (UIT T) a publié quelque 300 normes se rapportant à la cybersécurité. L'UIT fournit en outre une assistance aux pays en développement dans ce domaine et aide à la création d'équipes d'intervention en cas d'incident informatique (CIRT). Elle encourage également la coopération internationale dans le cadre de son Programme mondial cybersécurité[2].

Ce travail relève de la mission que les dirigeants du monde entier ont confiée à l'UIT lors des phases de 2003 et 2005 du Sommet mondial sur la société de l'information et qui consiste à encadrer la coordination de l'action internationale afin «d'établir la confiance et la sécurité dans l'utilisation des TIC».

---

[1] Voir aussi la Note d'information sur la Protection des infrastructures nationales essentielles.

[2] Voir www.itu.int/osg/csd/cybersecurity/gca/