Le cyberespace : *facteur de globalisation des risques*

Solange Ghernaouti

Internet a accompagné et favorisé le phénomène de mondialisation. Devenu omniprésent et incontournable, le cyberespace constitue désormais le prolongement technologique de notre environnement, c'est un écosystème régit par la loi du marché et les acteurs les plus forts. Ni pire ni meilleur, il reflète notre réalité sociale, économique et politique. Certains le considèrent comme le cinquième élément après la terre, la mer, l'air et l'espace. Comme ces derniers, il est l'objet de conquêtes et de convoitises. Moyen d'enrichissement, lieu d'expression du pouvoir, des crimes et des conflits, le cyberespace est un champ de bataille économique et politique à l'échelle mondiale.

Comme chaque technologie, celles constitutives du cyberespace possèdent leurs risques intrinsèques liés à un défaut de conception, de mise en œuvre, de gestion ou d'utilisation (usage détourné, abusif ou criminel). Ces risques sont majorés par notre dépendance aux technologies de l'Internet et par l'interdépendance globale de toutes les infrastructures informatiques mises en réseau ; y compris avec les infrastructures vitales au fonctionnement de notre société. Ainsi qu'il s'agisse des secteurs de la finance et de l'économie, de la santé ou de l'énergie par exemples, ces derniers dépendent des technologies de l'Internet.

Pour être opérationnel, le cyberespace consomme des ressources énergétiques considérables et produit des déchets augmentant ainsi les risques énergétique et environnemental. Des cyberattaques ciblées sur des systèmes de contrôle particuliers (traitement des eaux par exemples), peuvent avoir des impacts préjudiciables à la vie humaine, à la faune et la flore ou polluer.

Les criminels savent tirer partie des opportunités que leur offre Internet pour innover et être performant dans leurs activités classiques (trafics d'être humains, de drogue, chantage, extorsion, crime économique, blanchiment d'argent,…). Le mode de fonctionnement d'Internet, les problèmes de territorialité, d'entraide judiciaire internationale et le manque de moyens auxquels sont confrontés les instances de justice et de police pour poursuivre un crime transnational, profitent aux criminels. Internet offre une couche d'isolation protectrice, avec une relative impunité et une prise de risque minimale pour une profitabilité optimale.

Internet favorise à l'échelle planétaire, la mise en relation de cibles et de prédateurs, escrocs et malveillants de toute sorte qui agissent à distance, cachés derrière un écran. Le crime est automatisé, tout système connecté à Internet peut devenir une cible de la cybercriminalité. Chaque internaute peut être un criminel ou le devenir. Le passage à l'acte est facilité, y compris pour les plus jeunes, par la disponibilité et la dématérialisation des moyens et des victimes. Industrie et marché noir des outils de la cybercriminalité sont structurés autour de la mise à disposition de moyens et des compétences informatiques pour déstabiliser, prendre le contrôle, nuire ou s'enrichir. Certains sont disponibles gratuitement, d'autres à vendre où à louer. De la délinquance informatique au crime économique d'envergure, en passant par le harcèlement, la manipulation d'information, la surveillance ou l'espionnage, Internet est un vecteur amplificateur et de globalisation de la criminalité. Le risque informatique d'origine criminelle est ainsi devenu un risque structurel dont le coût est porté par la société.

Dans une société de l'information mondialisée, dans un contexte de crise économique et de compétition extrême, la guerre économique passe aussi par le cyberespace. Elle s'exprime par la manipulation de l'information, la fuite, le vol ou le détournement de données, par des filatures

numériques et l'espionnage. Influencer, porter atteinte à l'image et à la réputation des organisations et de leurs dirigeants, à la propriété intellectuelle, gagner des parts de marché, déstabiliser une organisation ou un état, tout cela est facilité par l'Internet.

Le secret numérique n'existe pas, l'intimité numérique est une illusion, les droits fondamentaux sont mis à mal, nous sommes tracés, suivis, observés, surveillés, géolocalisés, manipulables. Nos comportements, nos goûts, nos relations sont des marchandises. La prédation des ressources informationnelles, des savoirs faire, de la propriété intellectuelle, des données personnelles, le détournement des technologies à des fins commerciales ou malveillantes, sont une réalité. Cela autorise la montée en puissance de certains acteurs licites ou criminels et renforce leur hégémonie, au détriment de la souveraineté numérique des individus, des organisations et des états sur leurs patrimoines numériques. Le cyberespace est aussi vulnérables aux catastrophes naturelles, ce qui augmente les risques de non disponibilité ou d'intégrité des ressources qui le composent et d'altération de toutes les activités qui en dépendent.

Le risque « Cyber » est complexe et multiforme, il accentue tous les risques traditionnels, en génère de nouveaux tout en contribuant à la globalisation des risques. Il est devenu une urgence planétaire mondiale à prendre en considération.

Cet article a fait l'objet d'une publication dans le magazine WORK supplément Décembre 2013 de l'AGEFI (Agence Economique et Financière de Genève) (p. 22 – 23).

Solange Ghernaouti, Docteure en informatique de l'Université Paris VI, professeure de l'Université de Lausanne, experte internationale, Solange Ghernaouti est membre de l'Académie suisse des sciences techniques, directrice du *Swiss Cybersecurity Advisory and Research Group* (www.scarg.org), ancienne Auditrice de l'IHEDN, membre de l'ARCSI. Elle est l'auteure de nombreux ouvrages et publications scientifiques et de vulgarisation dont « *Cyberpower : crime, conflict & security in cyberspace* » (EPFL Press 2013), « La cybercriminalité : le visible et l'invisible » (Le savoir suisse, 2009). Elle fait partie des 20 femmes qui font la Suisse (Bilan 2012).