UQÀM | CHAIRE RAOUL-DANDURAND EN ÉTUDES STRATÉGIQUES ET DIPLOMATIQUES

CHRONIQUES DES NOUVELLES CONFLICTUALITÉS

@Leyre/Unsplash

Cyberattaques 2.0 : le risque devenu physique

Par Fanny Tan et Philippe Marchand

Le 23 décembre 2015, environ 230 000 Ukrainiens ont été plongés dans le noir à la suite de pannes d'électricité, qui ont duré jusqu'à six heures. Ce qui aurait pu être une interruption de service courante était en fait le résultat d'une cyberattaque massive orchestrée par le groupe russe Sandworm. Première cyberattaque réussie contre un réseau électrique révélée publiquement, cet incident braque les projecteurs sur un phénomène de plus en plus dangereux dans le paysage des cybermenaces : celui des attaques cyberphysiques.

Favorisées par la numérisation croissante des infrastructures physiques et des chaînes d'approvisionnement, ces attaques brouillent la frontière entre la sécurité physique et numérique. Elles font également planer le spectre d'une série de conséquences potentiellement dévastatrices pour la sécurité nationale. Dans un contexte géopolitique instable, quelles sont les vulnérabilités du Canada face à cette menace, et comment appréhende-t-il ce risque de plus en plus critique ?

Du virtuel au réel

Les attaques cyberphysiques peuvent être définies comme des cyberattaques entraînant des répercussions négatives sur l'espace physique, notamment les infrastructures critiques, telles que les usines de traitement des eaux ou encore les centrales électriques. Fréquemment qualifiée « d'émergente », cette menace préoccupe pourtant les gouvernements depuis longtemps. En effet, en 1996, avant même la démocratisation de l'Internet, les États-Unis publiaient un décret établissant le cyberterrorisme comme une menace pour les systèmes physiques, en particulier ceux des infrastructures critiques.

Si la menace des attaques cyberphysiques ne date pas d'hier, force est de constater que l'ère de la quatrième révolution industrielle, caractérisée par « une fusion des technologies estompant les frontières entre les sphères physique, numérique et biologique », ne fait qu'en accentuer la gravité.

Le consommateur peine désormais à échapper à cette fusion entre le monde « virtuel » et le monde matériel, en témoigne la montée en puissance des appareils connectés en tout genre (téléphone cellulaire, automobile, cafetière, réfrigérateur, toilette, etc.). Il en est de même du côté industriel avec le développement des systèmes de contrôle industriels accessibles depuis Internet, ainsi que la convergence des technologies opérationnelles et des technologies de l'information, connectant de surcroît les systèmes d'automatisation des opérations et de processus industriels à l'Internet. De plus, la priorisation du travail à distance au sein de nombreuses entreprises à la suite de la pandémie de COVID-19 entraîne une plus grande connectivité à Internet et augmente notre vulnérabilité.

Bien que cette révolution industrielle génère d'importants gains de productivité et d'efficacité, l'hyperconnexion qu'elle nécessite augmente considérablement la surface d'attaque des systèmes. En plus de procurer de nouvelles voies d'entrée aux systèmes physiques, l'intégration du numérique et de composantes connectées à l'Internet au sein des systèmes matériels accroît le nombre d'interconnexions entre les clients et génère de larges volumes de données, ce qui augmente la valeur des cibles aux yeux des acteurs malveillants. En visant certaines composantes essentielles au bon fonctionnement des infrastructures, les pirates informatiques peuvent diminuer leur efficacité, causer un bris temporaire ou encore les rendre inopérables.

Par exemple, en février 2021, un groupe non identifié a obtenu un accès non autorisé à un système américain de contrôle et d'acquisition de données en temps réel d'une station d'épuration d'eau. Les intrus ont pu augmenter la quantité d'hydroxyde de sodium dans l'eau, ce qui aurait pu causer une coupure de service temporaire.

Les secteurs critiques au Canada : qui est le plus à risque ?

Face à cette réalité, deux questions majeures émergent : quelles sont les cibles canadiennes les plus à risque de subir des attaques de ce type, et qui sont les acteurs les plus susceptibles de les perpétrer ?

Selon le gouvernement fédéral, trois cibles potentielles au sein des infrastructures essentielles sont particulièrement visées : les technologies opérationnelles, les chaînes d'approvisionnement et les systèmes de contrôle industriel accessibles depuis Internet. C'est d'ailleurs ce dernier type de système qui a été visé lors d'une récente attaque, révélée en octobre 2025, contre des secteurs critiques au Canada. Parmi les cibles touchées figurent une installation de traitement de l'eau, dont les valeurs de pression d'eau ont été trafiquées, et une entreprise pétrolière et gazière canadienne, qui a vu une de ses jauges magnétiques être manipulée, menant au déclenchement de fausses alarmes. Si le gouvernement demeure muet quant à l'origine et l'identité des attaquants, le terme utilisé, celui « d'hacktivistes », suggère une motivation politique derrière l'attaque.

Pour le gouvernement fédéral, les acteurs commandités par des États étrangers sont parmi les plus susceptibles de s'en prendre aux infrastructures critiques canadiennes — et encore plus largement à celles qui sont américaines. Des documents divulgués au printemps 2023 ont tout de même révélé qu'un groupe lié au Service fédéral de sécurité de la Fédération de Russie aurait réussi à pénétrer les infrastructures informatiques d'un opérateur de gazoduc canadien. Si le groupe affirme qu'il aurait été en mesure de saboter les systèmes de commande du gazoduc, il est permis d'en douter considérant la complexité d'une telle opération. Il pourrait plutôt s'agir d'une opération de reconnaissance en prévision d'une attaque ultérieure. Il est même possible qu'il ait tenté d'introduire ou d'attaquer les infrastructures énergétiques américaines via celles canadiennes compte tenu de leur grande interdépendance. Ottawa juge d'ailleurs improbable, en l'absence de conflit majeur et direct à l'échelle internationale, que des groupes commandités par des États tentent de perturber volontairement des systèmes critiques de manière à causer la perte de vies humaines.

Au-delà des acteurs aux motivations politiques et stratégiques qui viseraient à saboter les systèmes physiques pour attirer l'attention des médias, pour se prépositionner en cas de conflit ouvert ou pour recueillir de l'information stratégique, c'est d'abord et avant tout les acteurs aux motivations financières qui attirent l'attention du gouvernement fédéral. En effet, selon ce dernier, la majorité des attaques informatiques ciblant les infrastructures critiques canadiennes, comme le secteur de l'électricité, sont perpétrées par des groupes de rançongiciel. Leur méthode d'extorsion, qui consiste à prendre en otage des données ou à verrouiller des systèmes en l'échange d'une rançon, est fréquemment utilisée à l'encontre des infrastructures essentielles partout autour du monde.

Facilitée par la montée du modèle d'affaire du « rançongiciel-en-tant-que-service », la menace du rançongiciel s'amplifie et converge parfois avec les intérêts d'acteurs étatiques hostiles aux pays visés. Si cette dynamique accroît les risques pour les secteurs critiques, les conséquences physiques directes des attaques observées au pays demeurent, jusqu'à présent, limitées. Cette retenue semble liée non seulement à la recherche de gains financiers, mais aussi à la crainte d'une escalade : un sabotage matériel intentionnel pourrait effectivement être interprété, au regard des doctrines nationales et du droit international, comme un acte de guerre susceptible de provoquer des représailles majeures.

Le Canada est-il prêt à contrer la menace ?

Malgré les craintes d'attaques informatiques menant à des conséquences catastrophiques, un survol des dernières attaques cyberphysiques au Canada montre que celles-ci tendent à causer des interruptions ou des perturbations de service

(notamment, dans les secteurs de la santé, de l'alimentation et de l'énergie) plutôt que d'importants dommages matériels. Toutefois, la sophistication grandissante des différents acteurs du paysage de la menace (hacktivistes, cybercriminels et pirates commandités par les États), jumelée à une complexification et une connexion à l'Internet toujours plus grande des systèmes physiques au sein des secteurs critiques, laisse présager que ce type de menace continuera d'être sur nos radars dans les années à venir.

À l'heure actuelle, les mesures adoptées par le gouvernement canadien relèvent davantage de la recommandation que de l'obligation. Par exemple, la Stratégie nationale sur les infrastructures essentielles propose trois objectifs phares : l'établissement des partenariats; l'échange et la protection de l'information; et la mise en œuvre d'une approche de gestion tous risques. Bien que ces objectifs visent à assurer la résilience des infrastructures essentielles, elles n'impliquent pas d'obligations pour leurs propriétaires et exploitants, désignés par le gouvernement comme « les principaux responsables de la protection de leurs biens et services ». D'autres mesures données par le gouvernement, comme celles destinées à assurer la sécurité du réseau (notamment, via la restriction des appareils connectés à leur propre réseau, l'utilisation des phrases secrètes au lieu de mot de passe ou encore l'utilisation d'une authentification à deux facteurs), ou celles visant à promouvoir l'utilisation de technologies respectant le principe de « sécurisation dès la conception », sont, pour l'instant, des recommandations et non des obligations officielles.

La situation semble toutefois sur le point de changer. S'il devait être adopté, le projet de loi C-8 — actuellement en deuxième lecture à la Chambre des communes — obligera les exploitants de certaines infrastructures essentielles (comme le transport et les télécommunications) à élaborer rapidement un programme obligatoire de cybersécurité devant être révisé par le Centre canadien pour la cybersécurité et à déclarer une cyberattaque à celui-ci dans les 72 heures suivant l'incident. Le projet de loi exigera également des propriétaires et exploitants de certains secteurs à se conformer à diverses règles strictes en matière de sécurité, comme l'abandon de technologies jugées peu sécuritaires, sous peine d'amendes. En ce sens, le projet de loi C-8 rapprocherait le Canada d'un cadre formel de sécurité plus contraignant, tel que celui mis en place au fil des années par nos voisins du Sud.

Fanny Tan et **Philippe Marchand** sont chercheurs à l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand.

Pour en savoir plus sur la Chaire Raoul-Dandurand et ses travaux : https://dandurand.uqam.ca.

@Anton Maksimov/Unsplash