Agression électrique en Ukraine

Olivier Kempf

Le 23 décembre dernier, la petite ville d'Ivano-Francisk, dans l'ouest de l'Ukraine, a eu l'électricité coupée pendant quelques heures. N'accusez pas la vétusté, une sur-consommation, une grève ou toute autre explication qui vous viendrait à l'esprit : il s'agirait, d'après les autorités ukrainiennes, d'une attaque informatique contre la société exploitante. Surtout, cette agression aurait visé non l'informatique de gestion mais l'informatique industrielle, ce que les spécialistes appellent les SCADA (*Supervisory Control and Data Acquisition*), des systèmes spécialisés dans le contrôle des processus industriels. C'est très probable mais pas encore sûr à 100 %.
Le rapport d'une société de cybersécurité note « *une planification, une coordination et la capacité à utiliser des maliciels et probablement un accès à distance* » pour leurrer les systèmes. Il y aurait eu combinaison de plusieurs éléments pour réussir cette agression élaborée, ce qui suppose une organisation qui dépasse la simple injection d'un virus.

Sans surprise, les Ukrainiens (et beaucoup de commentateurs) ont désigné les Russes comme les auteurs de cette attaque. Remarquons cependant qu'aucun indice ne pointe directement vers une telle origine. Le mobile et la capacité technique ne suffisent pas à fournir la preuve d'un acte. De même, le fait qu'un des éléments de l'agression, le virus Blackenergy, ait été utilisé par un groupe de hackers contre l'OTAN en 2014 ne signifie pas que les mêmes l'aient réutilisé ailleurs. Aussi faut-il demeurer circonspect à l'endroit des accusations portées par les Ukrainiens, malgré le contexte troublé dans le pays, la persistance d'un séparatisme à l'ouest ou la capacité technique de la Russie. Celle-ci n'a pas intérêt aujourd'hui à relancer les hostilités en Ukraine et l'agression demeure somme toute assez limitée. Paradoxalement, le dénonciateur a plus intérêt à crier au loup que l'agresseur à couper le courant dans une petite ville quelconque. L'enjeu géopolitique n'est pas vraiment là.

Car l'affaire pointe l'attention vers ces SCADA et tout particulièrement sur ceux des réseaux électriques. Cela fait deux ans en effet que les spécialistes s'inquiètent de ces possibilités d'attaque. Rappelons pour mémoire que les premiers à les avoir mises en œuvre furent les Américains et les Israéliens, en lançant le virus Stuxnet contre une centrale nucléaire iranienne en 2010. Or, les mêmes Américains sont aujourd'hui fortement inquiets pour deux raisons : d'une part, leurs infrastructures électriques sont notoirement de faible qualité et mal protégées ; d'autre part, les États-Unis souhaitent promouvoir les « *smart grids* » ou réseaux électriques intelligents, associant l'informatique aux réseaux électriques. La question de leur sécurité apparaît cruciale.

La prise de conscience est générale. Vous avez ainsi peut-être entendu parler « d'infrastructures critiques ». Les Français négligent cet anglicisme pour s'intéresser au « Opérateurs d'Importance Vitale » (OIV). La dernière loi de programmation militaire leur impose ainsi des contraintes de cybersécurité beaucoup plus fortes car si l'affaire d'Ivano-Francisk paraît négligeable, elle annonce pourtant une cyberconflictualité à venir qui risque de décoiffer : imaginez-vous de vivre sans électricité ? Imaginez-vous de vivre sans ordinateur ? Imaginez-vous de vivre sans les deux ? Voici la question posée par la sécurité des SCADA.

Revue *Conflits*, avril-juin 2016 (2 juin 2016).