Le leurrage numérique et les mesures actives de cyberdéfense – une étude de cas suisse

Bastien Wanner[1], Solange Ghernaouti[2]

[1] Département des systèmes d'information, HEC Lausanne, Université de Lausanne
[2] Swiss Cybersecurity Advisory & Research Group, Université de Lausanne,
bastien.wanner@unil.ch

Résumé

Le leurrage numérique était initialement un ensemble de mesures dites passives et statiques disséminées dans une infrastructure informatique à surveiller et à protéger. Depuis, ce type de mesures c'est développé vers des actions plus actives et dynamiques. Dans la littérature, les mesures actives de cyberdéfense font référence à des actions – quasi-offensives – effectuées en dehors du périmètre de sa propre infrastructure informatique, en interaction avec l'adversaire et surtout cherchant à obtenir un effet, si possible perturbateur, au plus proche de la source d'une attaque afin de la faire cesser. Cet article a pour but de débattre si les leurres numériques peuvent être qualifié de mesures actives de cyberdéfense et d'analyser quels seraient les avantages et inconvénients d'une qualification "passives" ou "actives" ainsi que les opportunités et risques engendrés. L'analyse est complétée par une étude de cas issue de l'expérience suisse. Un éclairage particulier est apporté sur les obligations juridiques relatives à l'encadrement de ces mesures de cyberdéfense, notamment selon la loi fédérale sur le renseignement et la loi fédérale sur l'armée et l'administration militaire.

Mots clés :
cyber defence, active defensive measures, deceptive security