Entretien avec Thierry Berthier

Les hackers sont toujours sur une ligne de crête

Thierry Berthier, membre de la Chaire de cyberdéfense & cybersécurité Saint-Cyr, Sogeti, Thales

Août 2017 - Article II.5

ENTRETIEN - Marcus Hutchins, l'informaticien qui avait permis d'enrayer la cyberattaque mondiale de mai 2017, a été inculpé pour avoir fabriqué un logiciel malveillant. Thierry Berthier, maître de conférences en mathématiques et chercheur à la chaire de cybersécurité et défense de l'École spéciale militaire de Saint-Cyr, analyse l'ambiguïté entourant l'action des hackers. C'est pourquoi, après avoir rappelé les débats qui se sont tenus autour de l'hypothèse d'une iA toute puissante et malveillante, cet article propose une hypothèse intermédiaire : celle où une iA causerait, par mégarde, des désordres puis des catastrophes. Le scénario proposé envisage le déclenchement d'un conflit entre les alliés de l'oTAn et une puissance extérieure. Il vise à montrer qu'un des dangers de l'iA ne réside pas dans sa puissance (aujourd'hui entre deux géants américains du numérique hypothétique et donc fantasmée) ou dans son autonomie mais surtout dans les limites de sa puissance résultant d'un champ de pertinence très restreint. On ne développe à ce jour que des iA spécialisées, efficaces sur des problèmes limités et bien spécifiés mais strictement inopérantes sur des problèmes plus généraux. Le risque apparaît lors de la mise en résonnance involontaire de plusieurs iA spécifiques.

En général, les hackers sont toujours sur une ligne de crête. / Redpixel/stock.adobe.com

La Croix : **L'informaticien britannique qui avait permis d'enrayer la cyberattaque mondiale de mai 2017, Marcus Hutchins, a été inculpé aux États-Unis pour avoir fabriqué un logiciel malveillant. Comment expliquer cette ambivalence des hackers ?**

Thierry Berthier : Il existe une classification informelle des hackers, mais admise par eux. Aux extrêmes, on trouve les « White hat » (chapeau blanc), agissant pour la bonne cause, et les « Black hat » (chapeau noir), qui pratiquent la cybercriminalité. Entre les deux, les « grey hat » (chapeau gris) jouent sur les deux tableaux.

Marcus Hutchins pourrait être classé dans cette catégorie. Il est accusé d'avoir diffusé un logiciel malveillant. Cependant, il peut toujours mettre en avant qu'il visait uniquement à en trouver les failles. Pour trouver les vulnérabilités d'un système, il faut pouvoir entrer dedans. De ce fait, les hackers sont toujours sur une ligne de crête.

Existent-ils des lois sur les hackers ? Des moyens pour les ramener dans le système ?

T. B. : Certains pays, la France notamment, ont développé un large cadre juridique sur les questions de cyberdélinquance et de protection des données utilisateurs. Cependant, il n'existe pas d'uniformisation au niveau mondial, chaque État possédant ses propres lois.

Ces lois concernent par exemple des sociétés nées il y a une dizaine d'années, proposant des services de cybersécurité. Elles sont sollicitées par des grands groupes et des PME pour tester leur système informatique et en trouver les failles. C'est ce qu'on appelle des tests de pénétration. Ces sociétés vendent la découverte de vulnérabilités comme on vendrait du cacao ! Elles embauchent beaucoup d'anciens hackers. Ces nouveaux « white hat » y trouvent la possibilité d'une reconversion.

Un exemple emblématique est l'ancienne société française Vupen, spécialisée dans la détection de vulnérabilité des logiciels commerciaux tels que Microsoft. L'entreprise embauchait à la fois des informaticiens et des hackers. Du fait d'un cadre juridique très contraignant en France, l'entreprise a dû s'installer aux États-Unis. Elle a ensuite lancé la compagnie Zerodium, qui met en rapport les hackers et les éditeurs des logiciels commerciaux.

Les autorités publiques recherchent-elles également ce type de service ?

T. B. : Au niveau des autorités publiques, ce type de service est moins développé. Elles visent plutôt des ingénieurs spécialistes de la cybersécurité, sortis de grandes écoles ou d'une formation universitaire. Cependant, on manque de ce type de profils. Même si les universités ont développé des cursus, ceux-ci ne répondent pas encore, en termes de volumes, à la demande qui a explosé. Cette pénurie n'est pas particulièrement compensée par les hackers.

Recueilli par Claire Guyot