CYBERSÉCURITÉ UKRAINE RUSSIE

Les cinq points clés de la cyberguerre russe en Ukraine

Un large emploi d'armes numériques, qui évoluent au fil du temps, une défense qui a tenu le choc, grâce notamment aux acteurs privés, et des hacktivistes remontés à bloc un peu brouillon: bilan en cinq points de la cyberguerre qui fait rage en Ukraine depuis un an.

Gabriel Thierry

17 février 2023 \ 10h30

4 min. de lecture

Réagir →

© Max Kukurudziak/Unsplash

Il y a un an, l’armée russe lançait une offensive militaire majeure contre l’Ukraine, des opérations qui se sont traduites par des actions cyber. Mais quel bilan peut-on faire de ces opérations numériques? Voici un résumé en cinq points.

Des cyberarmes ont largement été employées

Comme le rappelait devant des députés le général Aymeric Bonnemaison, le patron de la cyberdéfense française, même s’il n’y a pas eu de "cyber Pearl Harbor", c’est-à-dire une opération numérique dévastatrice et spectaculaire, *"la cyberguerre a bel et bien lieu"* en Ukraine. Les actions de cyberguerre lancés par les russes sont en effet désormais bien documentées. Outre le piratage du satellite de communication Ka-Sat, dont le réseau était tombé en rade le 24 février 2022, il y a eu la diffusion dans les premières semaines du conflit de six différents Wiper, ces malwares destructeurs qui tentent d’effacer les données de leurs cibles, mais aussi de nombreuses opérations perturbatrices et d’une dizaine d’opérations de désinformation.

"Cela prend du temps et des ressources de concevoir un wiper bien ficelé, cela montre que la Russie n’a pas retenu

ses coups", observe le chercheur Alexis Rapin, qui travaille à l'université du Québec sur l'impact des technologies de l'information sur la sécurité internationale. Des actions qui avaient d'ailleurs commencé bien avant le 24 février. La société Mandiant, une filiale de Google, rappelle ainsi dans un récent rapport que les opérations cyber lancées en février 2022 ont été précédées d'une longue phase de plusieurs années d'espionnage et de pré-positionnement.

La cyberdéfense ukrainienne a tenu le choc

C'est la bonne nouvelle du conflit. "On présumait que dans le cyberespace l'attaquant aurait toujours l'avantage, remarque Alexis Rapin. On pensait qu'il était toujours plus facile de trouver des nouvelles portes d'entrées que de poser des serrures." Ce constat doit désormais être nuancé. La bonne cyberdéfense ukrainienne tient d'abord à une réorganisation en profondeur, ces dernières années, de leur dispositif. Les Ukrainiens avaient ainsi dévoilé une première stratégie de cyberdéfense en 2016.

"Ils ont fait leur révolution en montant en gamme, en créant une agence nationale et en ouvrant des budgets", listait Aymeric Bonnemaison devant la presse française à la mi-janvier. Mais ils ont également bénéficié de l'aide des experts du Cyber Command américain, quelques semaines avant l'ouverture du feu militaire, qui ont fouiné sur les réseaux pour rechercher les traces des hackers russes. Enfin, l'Ukraine a bénéficié du soutien de nombreuses entreprises occidentales spécialisées dans le numérique, de l'hébergement redondant de données à la fourniture de solutions de sécurité.

Un rôle des entreprises du numérique crucial

Ce soutien des entreprises du numérique est d'ailleurs l'un des points saillants du conflit. "On a l'impression que les acteurs privés du numérique deviennent moins timides à prendre une position de nature géopolitique, alors qu'ils avaient pu être mal à l'aise dans les années 2010 sur ce terrain-là", analyse Alexis Rapin.

Selon Mikko Hyppönen, directeur de la recherche chez WithSecure, ce serait même la première fois que des firmes de premier plan comme Microsoft ou Google interviennent directement dans un conflit. Leur action s'est

notamment concrétisée par des analyses fines sur les modes opératoires des attaquants russes, un partage de la connaissance crucial pour arrêter des actions malveillantes. L'un des responsables de la cybersécurité ukrainienne saluait ainsi récemment la coopération étroite mise en place entre les autorités publiques et le secteur privé. Une assistance qui va au-delà des Gafam, ces cinq entreprises emblématiques de la tech américaine. Le spécialiste slovaque de l'antivirus Eset avait ainsi fait partie des entreprises très actives dans la détection des wiper russes.

L'apport incertain des hacktivistes

Difficile par contre de se repérer dans la galaxie des groupes d'hacktivistes. Face à l'IT Army ukrainienne, un groupe emblématique qui a été un succès de communication au début du conflit avec plusieurs centaines de milliers de sympathisants, on retrouve désormais le collectif pro-russe Killnet. Mais, comme rappelé lors du dernier panorama de la cybercriminalité du Clusif, une association française de spécialistes de la sécurité, on dénombre derrière au moins 84 groupes d'hacktivistes mobilisés.

Au final, si le général Bonnemaison avait salué la montée en gamme de l'IT Army, il juge de manière générale que l'action "désordonnée" de ces différents groupes *"n'a pas été d'une grande efficacité"*. Outre de nombreuses attaques en déni de service, les hacktivistes se sont illustrés par des coups d'éclats aux lendemains incertains, comme ce piratage de la plateforme comptable de distribution d'alcool

Egais. *"On se demande si ces attaques hétéroclites et pléthoriques servent à quelque chose à l'échelle du conflit",* doute Alexis Rapin.

Des actions cyber qui se transforment

Même si on ne sait pas si Vladimir Poutine ne garde pas *"caché dans sa manche d'autres capacités"* cyber, comme l'avertissait Aymeric Bonnemaison, le conflit semble marquer une pause sur ce sujet. Il y a tout d'abord une première explication simple. Une fois les hostilités militaires ouvertes, pas besoin d'attaquer une centrale énergétique avec un précieux nouveau virus quand il suffit d'envoyer un missile. Les attaquants ont certainement eu besoin également d'un peu de temps pour concevoir de nouveaux programmes malveillants.

Enfin, c'est sans doute aussi l'illustration d'un changement d'outils. *"Les wipers étaient une bonne arme quand les russes croyaient encore pouvoir disloquer le dispositif ukrainien,* résume Alexis Rapin. *Pour ce chercheur, avec l'enlisement des opérations, les Russes semblent "rediriger des ressources vers les actions de désinformation"*. Une façon de tenter, en érodant le capital de sympathie occidental pour l'Ukraine, de faire levier sur l'importante aide militaire accordée à Kiyv.