LE CYBERESPACE MONDIAL EST MENACÉ LUI AUSSI

La bataille qu'on ne voit pas

Cyberattaques, intrusions sur les serveurs ennemis, logiciels malveillants et destructeurs de données. Manipulation des réseaux sociaux. Piratages d'activités sensibles comme les transports ou les hôpitaux. En marge du conflit armé sur le terrain, une guerre moins visible s'organise dans le cyberespace. Avec de possibles conséquences dans le monde réel, bien au-delà de la Russie et de l'Ukraine... CHRISTOPHE CHARLOT

Dette page n'est pas disponible pour le moment. *Page not found.* Cet avertissement bien connu des internautes se généralise ces derniers jours sur les sites internet les plus populaires ou les plus sensibles en Ukraine comme, désormais, en Russie. Et l'on ne parle bien sûr pas de problèmes de connexion. Ces indisponibilités sont le fruit d'intrusions, signes les plus visibles de la cyberguerre que se livrent la Russie et l'Ukraine en marge du conflit armé.

A l'ère du tout digital, rien d'étonnant en effet à ce que les combats se déroulent aussi sur internet. Mi-janvier déjà, l'Ukraine avait été la cible d'une cyberattaque de grande ampleur : 70 sites liés au gouvernement avaient été mis hors ligne tandis qu'un *malware* (logiciel malveillant) infiltrait de nombreuses organisations ukrainiennes, détruisant d'innombrables données, parfois sensibles.

Plus récemment, quelques jours avant le début des hostilités, de nouvelles attaques importantes ont également été menées dans le cyberespace, avec pour cible des serveurs étatiques et des sites web de référence en Ukraine : sites gouvernementaux (ministères de la Défense, de l'Intérieur ou des Affaires étrangères, par exemple), banques, médias, etc. Cette offensive a notamment pris la forme d'attaques DDos qui génèrent de très grands nombres de connexions sur un site, avec pour but de le faire crouler. Un *wiper*, logiciel qui efface des données sur les ordinateurs infectés, se serait aussi répandu en Ukraine.

Des groupes de hackers russes

Ces intrusions et destructions de données de grande ampleur participent à l'offensive générale et ont pour but d'engendrer le désordre, la crainte et l'insécurité chez un ennemi. Si rien n'est officiellement établi quant à l'origine de ces attaques, tous les regards se tournent évidemment vers le Kremlin, lequel n'a rien confirmé. Mais selon la BBC, un certain nombre d'offensives digitales proviendraient également de groupes de hackers patriotes russes qui s'introduisent sur les serveurs étatiques de l'Ukraine, génèrent des mails de *phishing*, détruisent des données et piratent les sites officiels. La crainte, c'est évidemment que ces attaques aillent un pas plus loin. "Aujourd'hui, quasi toutes les activités, y compris les plus sensibles, sont gérées de manière informatique, souligne un expert français. Aéronautique, hôpitaux, chemins de fer... Des intrusions pourraient rapidement créer le chaos." Ce ne serait pas une première : les citoyens ukrainiens ont subi de sévères perturbations et pannes électriques en 2015 et 2016, alors que son réseau électrique avait été la cible d'attaques, d'origine non établie


BELGAIMAGE

> **"Nous sommes en train de créer une armée informatique."** MYKHAÏLO FEDOROV, MINISTRE UKRAINIEN DU NUMÉRIQUE, DANS UN TWEET.

mais pour lesquels les soupçons se tournaient déjà vers Moscou. Et un peu plus tard, en 2017, le virus Notpetya avait paralysé le gouvernement et le système financier ukrainien avant de s'attaquer au reste du monde, causant des milliards d'euros de dégâts...

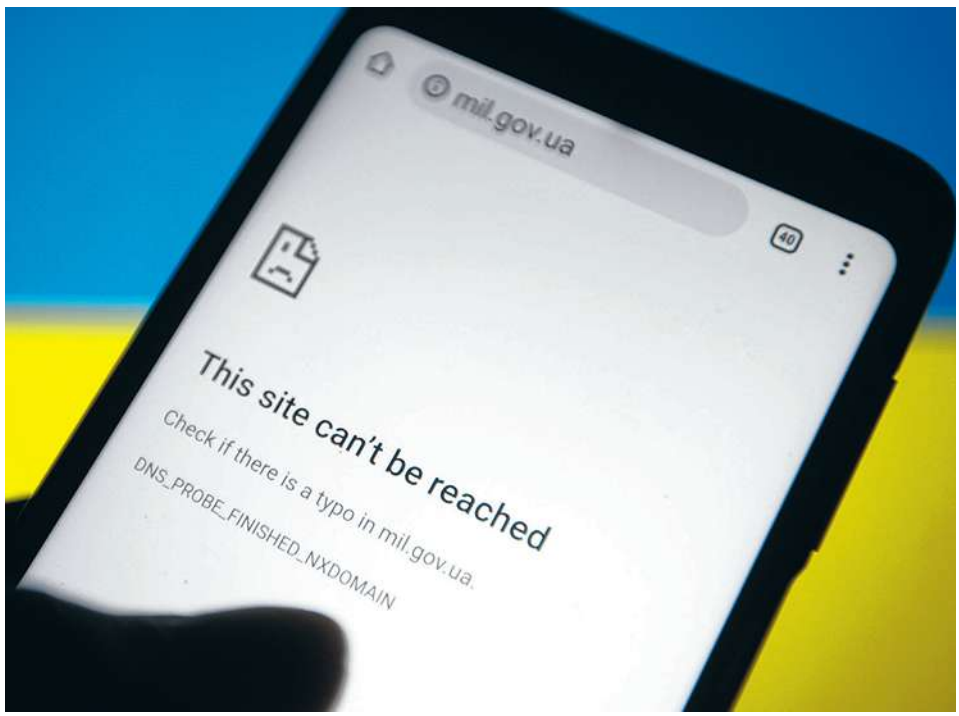
La cyber-riposte s'organise

A l'image du conflit sur le terrain, la riposte s'organise : les attaques se multiplient également à l'encontre des serveurs et des sites officiels russes. Le week-end passé, les sites du Kremlin, de la Douma et du ministère russe de la Défense étaient *down*. Une attaque revendiquée par le groupe de hackers Anonymous, qui aurait aussi piraté des sites de médias russes, faisant apparaître le message "Cette guerre n'est pas la nôtre. Arrêtons-la !". Des démarches soutenues, voire initiées par les autorités ukrainiennes : "Nous sommes en train de créer une armée informatique", a récemment tweeté Mykhaïlo Fedorov, le ministre ukrainien du Numérique, exhortant les férus d'informatique à rejoindre les rangs de cette armée virtuelle.

Le rôle des Gafa et des USA

Cet appel sur les réseaux n'est pas passe pas inaperçu, notamment sur les réseaux sociaux. Au point que les géants du net comme Facebook, Twitter, Google ou Apple ont été appelés à prendre certaines mesures ou les ont prises spontanément. Google a ainsi supprimé un certain nombre d'informations de sa cartographie pour éviter de "servir" l'armée russe : les conditions de circulation et des transports en commun en temps réel, par exemple, ou des données topographiques, ou celles des pistes cyclables... De leur côté, Facebook (souvent pris à partie pour son "rôle politique" dans les élections comme les conflits) et Twitter aident les Ukrainiens à verrouiller leurs profils et à protéger leurs communications.

L'implication des grandes entreprises américaines dans cette cyber-tension n'a rien d'anodin et témoigne de la globalité du conflit digital. Aussi, nombreux sont les observateurs qui s'attendent à une escalade et à des répercussions digitales ailleurs dans le monde. Les dirigeants américains et européens sont d'ailleurs en alerte face au risque d'attaques numériques qui pourraient cibler les pays ayant voté des sanctions contre la Russie. Les risques de cyberattaques, de piratages et de blocages en tous genres sont pris très au sérieux. Pour le sénateur américain Mark Warner, président de la commission du Sénat américain sur le renseignement, il est peu probable que les logiciels malveillants et les cyberattaques se limitent aux seules frontières de l'Ukraine. Les observateurs ont les yeux rivés sur les possibles cyber-actions américaines en la matière. Les services de sécurité américains auraient, selon NBC News, présenté à Joe Biden le plan d'une cyber-offensive massive en vue de perturber les actions militaires russes : coupures d'électricité ciblées, ruptures de connectivité du web en Russie, manipulations des aiguillages ferroviaires, etc. Une information formellement démentie par le gouvernement américain. Reste une crainte majeure : tout ce que les Etats-Unis feraient pourrait déclencher des ripostes numériques sans précédent et une escalade vers une nouvelle forme de guerre mondiale...



GETTY IMAGES

GUERRE VIRTUELLE
Il est peu probable que les logiciels malveillants et les cyberattaques se limitent aux seules frontières de l'Ukraine.