Document 1 La cyberguerre en Ukraine est aussi cruciale que la bataille dans les tranchées

« Rien ne permet de savoir qui se trouve à l'intérieur de l'immeuble de bureaux de Kiev, mais les Russes n'ont pas besoin d'une plaque d'identification pour le savoir. Les fenêtres des étages supérieurs sont encore brisées à la suite d'une attaque de drone l'été dernier contre le centre névralgique des opérations de cyberdéfense de l'Ukraine. Les deux parties sont engagées dans un combat pour voler des renseignements et semer la panique en attaquant les télécommunications, les infrastructures critiques, les ordinateurs militaires et tout ce qu'elles peuvent pirater.
Cette guerre se déroule dans l'ombre, affirme un responsable des services de renseignement ukrainiens. En juin dernier, dit-il, de « grandes frappes » ont entraîné la fermeture de stations-service et de fournisseurs d'accès à Internet dans les régions russes de Belgorod et de Rostov, mais peu d'étrangers l'ont remarqué et les autorités russes n'ont rien dit à ce sujet. Tim Karpinsky, directeur de l'Ukrainian Cyber Alliance, une « communauté d'hacktivistes », explique que de nombreux Ukrainiens et Russes, y compris de vastes réseaux criminels, travaillaient autrefois ensemble dans les domaines de l'informatique et de la cybernétique. Lorsque les deux pays sont entrés en guerre, cela signifiait que les Ukrainiens avaient « les compétences, les outils, les connaissances et les capacités nécessaires pour riposter efficacement ». Les cyber-guerriers se voient combattre sur une nouvelle ligne de front, aussi cruciale que la guerre dans les tranchées.

Les grandes attaques russes d'il y a dix ans ont servi de signal d'alarme. En 2015, des pirates informatiques ont infiltré les systèmes des centrales électriques et coupé l'électricité pendant plusieurs heures dans certaines régions de l'ouest de l'Ukraine. Le réseau de Kiev a été attaqué un an plus tard. En juin 2017, les ordinateurs des banques, des compagnies d'énergie et du gouvernement ont été attaqués, écrit un analyste, David Kirichenko, dans un nouveau rapport. Les données de 10 % des ordinateurs ukrainiens ont été effacées, dit-il, ce qui a entraîné une perturbation généralisée.

Selon Dmytro Osyka de Modus X, la branche cybersécurité de dtek, qui produisait environ un quart de l'énergie ukrainienne avant l'invasion de 2022, l'une des conséquences est que personne ne peut désormais s'introduire dans les commandes de ses centrales électriques, car elles ont été mises hors ligne et isolées du reste de l'infrastructure cybernétique de l'entreprise. Depuis l'invasion, l'équipe de cyberdéfense de dtek a quadruplé pour atteindre 40 personnes.
Volodymyr Korniichuk dirige la sécurité de Diia, une application utilisée par 20 millions d'Ukrainiens, qui contient leur carte d'identité et d'autres documents et leur permet de payer leurs impôts, d'obtenir des prestations de sécurité sociale, etc. « Il n'y a pas une semaine où nous n'avons pas été attaqués », déclare-t-il. Lors d'une opération russe, on a découvert une société qui avait été constituée deux semaines avant l'invasion. Elle est remontée jusqu'à l'adresse d'une société enregistrée à Londres.
En décembre, lors de la plus grande attaque réussie de la guerre, des pirates informatiques russes ont mis hors service Kyivstar, le plus grand fournisseur de téléphonie mobile et d'accès à Internet d'Ukraine, interrompant les services pendant plusieurs jours. Debout devant un grand écran, le major Yurii Myronenko, chef du Service national des communications spéciales et de la protection de l'information de l'Ukraine (SSSCIP), montre des graphiques détaillant les responsables. Le SSSCIP relève des services de sécurité, il est donc en uniforme. Il est également au centre d'une galaxie d'organismes de cyberdéfense étatiques, militaires et privés, qu'il aide à coordonner. En 2022, il y a eu 2 194 « cyberincidents », dont 1 048 étaient « majeurs ou critiques ». En 2023, il y en a eu 2 554, dont 367 seulement étaient graves. Les cyberdéfenseurs ukrainiens ont donc considérablement réduit le taux d'attaques graves. Mais au cours des deux premiers mois de l'année, les Russes ont intensifié leur action, et M. Kovalev s'attend à ce que l'année 2024 soit « encore plus difficile en termes de cyberguerre ».

Il explique que le SSSCIP a appris que 10 % des attaques proviennent des cyberunités des services de sécurité russes, tandis que le reste est le fait de groupes de pirates informatiques criminels affiliés et autres. L'unité cybernétique russe la plus efficace s'appelle Armageddon et appartient au service de sécurité du FSB. Certains de ses membres seraient d'anciens membres des services de sécurité ukrainiens en Crimée qui ont fait défection vers la Russie lors de l'annexion de la péninsule en 2014.

M. Kirichenko explique que lorsque l'invasion de 2022 a commencé, les experts ont craint un « Pearl Harbour numérique » ; mais les défenses de l'Ukraine ont remarquablement « tenu bon ». Aujourd'hui, prévient-il, « la cyberguerre entre la Russie et l'Ukraine devient plus agressive que jamais et continuera à s'étendre à l'avenir à des cibles critiques potentiellement plus dévastatrices ».

Source : challenges.fr, 27/03/2024

Document 2

« [Les Ukrainiens] développent depuis quelques années des capacités de défense de leurs systèmes. Et quelques jours avant la guerre, ils ont reçu l'aide précieuse des États-Unis, affirme le chercheur Julien Nocetti : *"Il y a eu des coopérations denses entre Kiev, l'Otan et les États-Unis pour muscler la cyberdéfense et la résilience des infrastructures ukrainiennes en amont du conflit. On constate un resserrement des liens de coopération entre le renseignement américain, la NSA, et les Ukrainiens."* Les Européens aussi ont envoyé des experts dans les premières heures du conflit.

À cela s'ajoute le soutien de bénévoles du monde entier. Deux jours après le début de l'invasion russe, le ministre ukrainien de la Transformation digitale a annoncé la création d'une armée numérique ou "IT army". Des milliers de personnes du monde entier ont alors rejoint un forum de discussion sur la messagerie Telegram, afin d'attaquer certaines cibles russes, sites gouvernementaux ou autres. Aujourd'hui, ces pirates bénévoles vont jusqu'à identifier et contacter les familles de soldats russes qui combattent en Ukraine, pour les prévenir des agissements de leurs proches. Un champ d'action très large pour tenter de perturber au mieux l'offensive russe.

Ces actions ne sont pas sans risque, prévient cependant Rayna Stamboliyska : "*Les personnes qui mènent ces attaques n'ont aucun mandat officiel autre que la réponse à un tweet et la participation à un groupe Telegram. Ce sont des Ukrainiens, mais aussi des Américains, des Français, des Danois, et ils font de l'intrusion. Ils sont donc en situation d'infraction." » (…)*

"Connaître l'objectif de ces attaques est toujours compliqué, précise François Deruty, l'ancien sous-directeur Opérations de l'Anssi. On trouve des codes malveillants mais tant qu'on ne sait pas s'il s'agit simplement d'espionner les communications ou de les détruire on ne se rend pas bien compte de l'effet final recherché. Et c'est compliqué de remonter jusqu'au commanditaire."

L'Anssi avait publié une note sur le sujet à l'époque, mais sans jamais mentionner la Russie. *"La doctrine française consiste à ne pas désigner publiquement les coupables comme le font d'autres pays*, poursuit François Deruty. *On peut en discuter en bilatéral, on peut utiliser le canal diplomatique. Il y a d'autres façons de pointer du doigt ou de faire savoir qu'on est au courant de certaines choses."* Selon nos informations cependant, la Russie semble bel et bien derrière ce dépôt d'implants. Un groupe criminel nommé Energetic Bear, proche de Moscou et repéré aussi aux États-Unis sous d'autres noms, serait derrière ces attaques.

Face à ces craintes, la France se prépare. L'Anssi a publié une note dès le début de la guerre pour demander aux entreprises françaises de se protéger. Sont particulièrement surveillés les opérateurs d'importance vitale (ministères, centrales nucléaires…) surtout à l'approche de grands événements comme la Coupe du monde de rugby de 2023, ou les Jeux olympiques de 2024. L'armée aussi se prépare. Elle a tenu son crash-test annuel : une simulation de cyberattaques pour faciliter le fonctionnement de la chaîne de commandement. Cette année, le thème de l'exercice était *"un pays exclu des Jeux olympiques décide d'envahir une région frontalière d'un État allié de la France"*. Le sous-entendu est clair.

Source : Maxime Fayolle, *Cyberguerre : la Russie jusqu'à présent tenue en échec par l'Ukraine,*francetvinfo, 9 avril 2022

Document 3

« Depuis quelques années, la cyberguerre profite d'un terreau d'expansion très favorable. Certains pays ont lancé leur programme de création d'« *unités cyber* ». Ainsi la Chine, la Syrie, les États-Unis ou la Grande-Bretagne ont largement investi dans la mise sur pied de *cyberbataillons*. La prise de conscience des Chinois face à l'obsolescence technologique de leurs équipements militaires dans les années 1990 a accéléré la recherche d'une vulnérabilité qui leur permettrait de devancer les États-Unis. Cette vulnérabilité réside notamment dans la dépendance des nations occidentales aux technologies de l'information. La création d'un corps d'armée cyber de 9 600 hommes par la Chine, dont les unités 61 398 et 61 046, répond clairement à la volonté de mener une guerre dans le cyberespace. (…)

Les cyberattaques sont-elles destinées à faire partie d'une panoplie de techniques soumettant l'adversaire à sa volonté et menant à la victoire ? Les moyens déployés récemment par la Russie en Ukraine s'apparentent à un nouveau genre de guerre dite non-linéaire ou hybride, qui implique de multiples acteurs : médiatiques, diplomatiques, humanitaires, économiques, d'influence, mercenaires. L'emploi combiné de ces moyens s'apparente à une interpénétration de *soft* et *hard power*. (…)

Le principe stratégique de concentration des efforts implique de porter l'effort en un certain point avec un maximum de forces. L'intérêt de la cyberguerre est de se concentrer là où n'opère pas la force militaire. Des frappes conventionnelles peuvent se dérouler sur un secteur, alors que les moyens de cyberguerre peuvent opérer ailleurs. (…)

Tactiquement, au niveau des unités de combat, il est encore délicat de mettre en pratique la guerre numérique. Si la littérature militaire développe des théories nouvelles sur l'usage des moyens informatiques (...), la réalisation concrète du combat numérique généralisé par les unités au contact n'est pas encore à l'ordre du jour. L'armée de Terre utilise des unités légères de guerre électronique qui interviennent en opération. Sur ce modèle, des unités de combat numérisées dûment formées et équipées pourraient un jour compléter l'arsenal militaire tactique.»

Source: LUIGGI Jean-Sun, « Cyberguerre, nouveau visage de la guerre ? », Stratégique, 2016/2 (N° 112), p. 91-100. DOI : 10.3917/strat.112.0091. URL : https://www.cairn.info/revue-strategique-2016-2-page-91.htm