LE RUBICON

Des bitcoins aux missiles : en Corée du Nord, un cyber-banditisme d'État

Alexis Rapin | 21 novembre 2024

Contrairement à ce que dépeignent certains films hollywoodiens, on n'achète pas facilement un arsenal nucléaire avec des valises de billets. Avec de la cryptomonnaie, toutefois, c'est peut-être une autre affaire. Depuis une dizaine d'années maintenant, la Corée du Nord s'appuie de plus en plus sur la cybercriminalité, et notamment le vol de cryptomonnaies, pour financer son programme balistique. En dépit de sanctions internationales écrasantes, la République populaire démocratique de Corée (RPDC) s'est rendue maitre dans l'art du piratage de banques et de *crypto exchanges*, parvenant ainsi à maintenir le régime à flot et à poursuivre le développement de missiles de longue portée. Selon certaines estimations, depuis 2017, les hackers de Pyongyang auraient dérobé l'équivalent de 3 milliards de dollars en seules cryptomonnaies, assurant ainsi le financement de près de la moitié de son programme balistique.

Là où certains experts voient dans le conflit en Ukraine un signe que le cyber peine à livrer ses promesses aux niveaux opératif et tactique, la Corée du Nord incarne au contraire l'exemple d'un État étant adroitement parvenu à mettre le cyber au service de ses priorités géopolitiques. Si dans les prochaines années la Corée du Nord parvient finalement à s'équiper de missiles à même de frapper le continent américain, tout indique que le cyber aura joué un rôle majeur dans ce tour de force. Au-delà des questions de prolifération, ce phénomène pose aussi évidemment ses propres enjeux sécuritaires, en matière ou de sureté de l'industrie financière par exemple.

Recourant à des méthodes et des circuits en tout point similaires à ceux des groupes cybercriminels, la Corée du nord dessine ainsi un modèle d'emploi du cyber qui, s'il a pu connaître des précédents isolés, s'avère unique par son échelle et son degré de maturité. Pour autant, alors que l'usage de sanctions économiques connaît une croissance marquée sur la scène internationale, d'autres régimes, isolés et manquant de sources de revenus, pourraient être tentés de s'en inspirer à l'avenir. Face à ce qu'il convient d'appeler un cyber-banditisme d'État, il apparaît important de comprendre comment le modèle nord-coréen a vu le jour et s'est sophistiqué au fil du temps, afin de mieux cerner non seulement sa portée mais aussi son potentiel de propagation.

De la planche à billets aux braquages numériques

Économiquement asphyxiée depuis de nombreuses années, la Corée du Nord n'en est pas à son coup d'essai en matière de circuits de financement clandestins. Entre les années 1970 et 2000, la RPDC aurait notamment recouru au faux-monnayage, à la contrebande de cigarettes ou même à la contrefaçon de viagra pour remplir les coffres du régime. C'est toutefois au milieu des années 2010 que le royaume ermite saisit le potentiel des cyber opérations en la matière. Une vaste cyberattaque menée en 2013 contre différentes banques (et médias) sud-coréens livre un premier signal que les hackers de Pyongyang lorgnent du côté de l'industrie financière, à ce stade dans une volonté de perturbation et non pas d'enrichissement.

C'est la Banque centrale du Bangladesh qui, en 2016, sera la première cible d'une cyber-opération nord-coréenne à but foncièrement lucratif. Compromettant le système de transfert SWIFT de l'institution, les pirates font discrètement ordonner 35 versements via la réserve fédérale de New York, totalisant près d'un milliard de dollars. Du fait d'un coup de chance et d'une faute de frappe, la supercherie est repérée de justesse par un employé de la Fed, trop tard néanmoins pour empêcher une partie de la transaction (81 millions) à destination d'une banque philippine. L'essentiel du magot est par la suite récupéré en cash puis prestement blanchi dans des casinos de la région de Manille. Aux yeux de Pyongyang, l'opération vient sans doute démontrer que le cyber peut produire en quelques mois la manne que de complexes réseaux de contrebande prenaient auparavant plusieurs années à générer.

Sans surprise, le schéma est reproduit (sous des formes variées) à de nombreuses reprises par la suite. En 2018, c'est l'institution indienne Cosmos Bank qui se voit soutirer 11 millions de dollars. L'année suivante, à Malte, les Nord-Coréens dérobent 14 millions à la Bank of Valletta. En 2017, la firme de cybersécurité Kaspersky révèle qu'au moins 18 pays ont déjà vu des institutions financières visées par des cyberattaques nord-coréennes.

La même année, les pirates de Pyongyang s'essaient à une nouvelle technique de brigandage : les rançongiciels, des virus chiffrant les données d'un ordinateur pour exiger une rançon en échange d'une clé de décryptage. En mai 2017, le *ransomware* WannaCry se répand comme une trainée de poudre à travers le monde, infectant en une journée 230 00 machines dans près de 150 pays. Comme bien d'autres pirates, les Nord-Coréens ne restituent aucun accès aux victimes s'acquittant de la rançon demandée et WannaCry ne ramène en définitive que 300 000 dollars à ses auteurs. L'épisode n'a toutefois pas découragé l'usage des rançongiciels par les hackers de la RPDC, qui étaient observés prendre pour cible des entreprises américaines en octobre 2024 encore.

Lazarus Group, braqueurs en série

Si l'on en croit les attributions émises par diverses entreprises de cybersécurité et agences gouvernementales au fil des ans, l'essentiel des opérations susmentionnées sont à mettre au crédit d'un seul et même acteur : Lazarus Group, une unité de pirates informatiques rattachée au 3e Bureau du Bureau général de reconnaissance (RGB) de l'Armée populaire de Corée. Lazarus serait actif depuis 2009 au moins, lorsqu'il aurait fait ses premières armes en conduisant des attaques par déni de service contre des organisations sud-coréennes. Certains experts en cybersécurité estiment cependant que derrière le nom (communément utilisé) de Lazarus se cacheraient en fait plusieurs groupes différents, répartis dans différentes sous-sections du 3e Bureau et assumant des missions distinctes.

Monolithique ou non, Lazarus ne représente qu'une partie des forces cyber que le régime nord-coréen a patiemment bâti au fil des ans. La création et le maintien de cette petite armée, actuellement estimée à 8 400 individus, représente un véritable tour de force pour le pays le moins connecté au monde. Nombre de ces pirates opéreraient sous couverture depuis des pays tiers (comme la Thaïlande, la Malaisie et surtout la Chine voisine), où l'infrastructure numérique est infiniment meilleure et où la profusion d'utilisateurs, de servers et d'adresses IP permet une meilleure dilution d'activités numériques clandestines. Les villes chinoises de Dalian et Shenyang, proches de la frontière nord-coréenne, seraient d'importantes bases opérationnelles des pirates de la RPDC. Ceux-ci s'y feraient notamment passer pour de simples travailleurs du domaine des TI, à grand renfort de sociétés écran créés à cette fin par Pyongyang.

Si la firme de cybersécurité Recorded Future estime que près des deux tiers de l'activité cyber nord-coréenne relève en définitive de collecte de renseignement, Lazarus semble le groupe de pirates le plus focalisé sur les attaques à but lucratif. Bien que les États-Unis soient pour l'heure parvenus à identifier (et inculper) quatre membres du groupe, la taille et la composition exacte de celui-ci restent nébuleuses.

Le virage crypto

Alors que les efforts de cyber-banditisme nord-coréens se sont surtout concentrés, entre 2016 et 2019, sur les banques et l'industrie financière traditionnelle, un virage important s'est opéré depuis. De fait, le secteur des cryptomonnaies est aujourd'hui devenu la cible première des pirates nord-coréens. L'enchainement des coups de main menés par Pyongyang au fil des ans a d'ailleurs de quoi donner le vertige : 275 millions subtilisés à KuCoin en 2020, 100 millions soutirés à Harmony puis Atomic Wallet en 2022 et 2023, 190 millions entre temps dérobés à Nomad. Dans son dernier rapport publié en mars 2024, le Groupe d'experts des Nations unies sur les sanctions visant la RPDC disait avoir déjà recensé un total de 58 cyberattaques nord-coréennes ayant visé le secteur de la cryptomonnaie. Le record du plus gros larcin est actuellement détenu par Axie Infinity, qui s'est vue soulagée de 620 millions par Lazarus en 2022.

Le choix de cibler l'industrie de la crypto s'explique assez facilement. D'une part, le caractère pseudonyme des transactions par blockchain, et la difficulté de retracer certaines chaines de transaction complexes (transitant par de nombreuses juridictions par exemple) compliquent les efforts d'investigation et jouent donc à l'avantage des pirates. D'autre part, le secteur reste à ce stade surtout constitué d'entreprises de taille modeste, soumises à des régulations le plus souvent limitées, et ne disposant dans bien des cas que d'un personnel de sécurité restreint (comparativement aux géants de la finance). Les acteurs de la crypto font ainsi figure de « cibles molles » pour la RPDC. Qui plus est, la variété des systèmes, langages et protocoles coexistant actuellement dans l'industrie de la crypto accroît d'autant le potentiel de vulnérabilités logicielles, et donc la surface d'attaque à la disposition des hackers.

Pour autant, le blanchiment et le retrait des sommes dérobées demeurent un défi majeur pour la RPDC, et tout indique qu'une fraction seulement des millions détournés par ses hackers ne finit véritablement dans les coffres du régime. De fait, des efforts considérables sont déployés par les agences de sécurité étatiques pour retracer, saisir et restituer les cryptomonnaies subtilisées. Ironiquement, la communauté de la cryptomonnaie, empreinte d'une forte idéologie libertarienne voire anti-étatiste, s'avère pour l'heure largement dépendante du FBI et de ses pairs pour assurer sa sécurité. Si pour l'heure les actions anti-blanchiment sont probablement le volet le plus fructueux de la lutte menée au cyber-banditisme nord-coréen, reste que l'appétit de Pyongyang ne tarit pas : les plus récentes estimations indiquent que les hackers nord-coréens ont conduit 20 piratages de cryptomonnaies en 2023, pour un butin équivalent à un milliard de dollars.

Un potentiel évolutif inachevé

Il importe de noter que les pirates de la RPDC ne cessent d'innover et de raffiner leurs techniques de financement clandestin. Depuis 2022, la Corée du Nord multiplie notamment les tentatives de faire discrètement embaucher de ses agents comme travailleurs à distance dans les services de TI de grandes firmes occidentales. Masquant leur identité et leur origine derrière des photos générées par IA et des sociétés écran, ceux-ci ont pour rôle premier de reverser leur salaire au régime, mais transmettent aussi fréquemment des accès numériques aux hackers du renseignement. Ces derniers peuvent alors monter des opérations de fraude ou collecter de l'information sensible.

Si les *crypto exchanges* font actuellement figure de victime principale de Lazarus et consorts, ceux-ci pourraient dans l'absolu n'être qu'une cible d'opportunité passagère. Alors que les hackers nord-coréens ont par le passé déjà habilement instrumentalisé l'industrie du jeu vidéo payant, certains observateurs notent que la popularité croissante des plateformes de jeu vidéo « play-to-earn » (P2E) pourrait prochainement susciter l'intérêt de Pyongyang. D'autres institutions ou mécanismes financiers émergents, comme les apps de paiement mobiles ou les systèmes de paiement en temps réel, pourraient également se retrouver demain dans le collimateur des hackers de la RPDC s'ils s'avèrent efficacement exploitables à grande échelle.

En d'autres termes, le cyber-banditisme d'État nord-coréen est loin d'avoir épuisé ses « possibilités évolutionnaires ». Parallèlement, les effectifs des forces cyber du royaume ermite auraient augmenté de 20% sur les deux dernières années, et le nombre d'opérations (repérées) contre le secteur de la crypto augmente de manière constante depuis 2020. Tout porte donc à croire que le cyber-banditisme de la RPDC va aller croissant à court voire moyen-terme.

Facteur de prolifération, gage d'instabilité

Si l'on en croit les rapports produits par le Groupe d'experts des Nations unies sur l'application des sanctions à l'encontre de la RPDC, les activités cyber de Pyongyang contribuent très directement aux progrès affichés par son programme nucléaire. En sus des importants revenus générés par les pirates (représentant 40% du financement du programme, selon le dernier rapport du Groupe), le volet espionnage des activités cyber nord-coréennes consacre d'importants efforts à dérober des secrets nucléaires et balistiques en Occident et au-delà. Andariel, un autre groupe de pirates rattaché au Bureau général de reconnaissance, aurait dans les dernières années visé notamment des centrales et laboratoires de recherche nucléaire, des entreprises de l'aérospatiale, ou encore le secteur naval (dans le but notamment de développer la composante sous-marine de l'arsenal

nucléaire de la RPDC). Le cyber représente donc, à différents égards, une sorte d'appendice du programme nucléaire nord-coréen.

Pour autant, le cyber-banditisme de la RPDC soulève également ses enjeux propres. D'une part, il introduit un nouveau mécanisme de contournement de sanctions économiques, qui vient questionner encore davantage leur efficacité en tant que moyen de pression géopolitique. Il instaure de surcroît une méthode clandestine de financement pour des États ou acteurs n'ayant pas de rentes importantes à faire valoir – contrebande de pétrole, trafic de pierres précieuses, par exemple.

D'autre part, il peut également représenter un facteur d'instabilité significatif pour le secteur financier dans son ensemble. Fin 2017, la firme de gestion de cryptomonnaie sud-coréenne Youbit a été forcée de mettre la clé sous la porte après s'être fait subtiliser 17% de ses actifs par des hackers, que beaucoup soupçonnent nord-coréens. Il n'est pas inconcevable qu'une opération similaire contre un acteur majeur du secteur puisse un jour créer une onde de choc sur les marchés financiers, et affecter un circuit économique plus vaste. Se pose aussi la question de savoir si le cyber-banditisme étatique pourrait à l'avenir se doubler d'objectifs autres que lucratifs. Un État, en sus de remplir ses coffres, pourrait par exemple chercher à affaiblir des entreprises spécifiques faisant concurrence à ses fleurons nationaux sur des marchés stratégiques. L'enjeu pourrait également être de rançonner une entreprise pour la décourager d'entreprendre certaines actions indésirées (à l'instar de l'attaque nord-coréenne menée en 2014 contre Sony Pictures pour empêcher la sortie du film *The Interview*). Au-delà de l'enjeu de la prolifération, le cyber-banditisme d'État représente donc également un facteur d'insécurité en soi.

Un modèle unique… pour toujours?

La Corée du Nord n'est pas le seul État dans lequel des liens entre structures de pouvoir et cybercriminalité ont été documentés : la Russie et l'Iran, pour ne citer qu'eux, témoignent de divers mécanismes de connivence plus ou moins structurés entre appareil gouvernemental et hackers criminels. Le cas nord-coréen est toutefois singulier, en ce que c'est l'État lui-même qui entraine et encadre des pirates informatiques ayant pour mission spécifique de mener des cyberattaques à but lucratif. Il ne s'agit pas, comme en Russie, de liens informels dans lesquels des groupes cybercriminels menant une existence propre sont tenus de collaborer occasionnellement avec les services de sécurité. Il ne s'agit pas non plus d'arrangements circonstanciels, dans lequel des acteurs cyber sont tacitement autorisés à s'enrichir illégalement en marge d'activités à visée stratégique (comme cela a déjà pu être constaté en Chine par exemple). Le recours au cyber-banditisme est ici une politique à part entière, menée par et pour l'État nord-coréen.

Ce modèle est évidemment le fruit de conditions bien particulières. D'une part, la Corée du Nord est un État lourdement sanctionné, diplomatiquement isolé, économiquement peu diversifié, en mal de devises. D'autre part, le régime nord-coréen nourrit une idéologie ouvertement révolutionnaire et anticapitaliste, qui appelle à retourner contre les puissances libérales les outils et structures qu'elles ont créés. Alors que le régime interdit et punit sévèrement l'usage d'internet, présenté comme un cheval de Troie occidental, il revendique parallèlement volontiers son utilisation stratégique pour lutter contre les ennemis de la RPDC. La conjonction d'un dénuement économique quasi-structurel et d'un rejet assumé des normes internationales libérales constituent ainsi les principaux catalyseurs du cyber-banditisme d'État nord-coréen.

Ces circonstances sont-elles uniques, et appelées à le rester? La question mérite d'être posée. De fait, le modèle de cyber-banditisme nord-coréen constitue à ce jour un succès indéniable, qui pourrait inspirer d'autres acteurs dans une situation comparable. Le Myanmar, le Venezuela [1][2] ou encore la Biélorussie, par exemple, réunissent actuellement différentes conditions pouvant constituer un terreau fertile à l'émergence d'un cyber-banditisme d'État : une situation économique difficile, des sanctions importantes à leur encontre, un régime peu attaché aux (voire contestant ouvertement les) normes libérales, et surtout un écosystème cybercriminel préexistant et bien organisé. Sans qu'il ne soit intégralement créé de la main de l'État, à l'instar du cas nord-coréen, un « système cyber-banditiste » pourrait émerger au terme d'une convergence ou d'une cooptation des réseaux criminels par les structures de pouvoir. Il va sans dire que le modèle présente également un attrait majeur pour des acteurs non- ou semi-étatiques, et pourrait par exemple devenir prochainement un mécanisme de financement du terrorisme (à l'instar du rôle joué par la piraterie pour certains groupes armés somaliens).

Ainsi, on aurait probablement tort d'aborder le cyber-banditisme d'État nord-coréen comme une simple nuisance ou un épiphénomène géopolitique. Celui-ci constitue une politique de puissance à part entière, mobilisant (et confisquant) des ressources considérables sur la scène internationale, et qui pourrait à l'avenir servir de modèle à d'autres acteurs. Différents modes d'action sont déjà mis à contribution pour tenter d'endiguer le phénomène : lutte au blanchiment pour priver les hackers des fruits de leurs larcins, et démantèlement d'infrastructures informatiques pour entraver leurs opérations, entre autres. Pour autant, l'essor continu des cyberattaques nord-coréennes suggère que les ressources allouées à ces contre-mesures restent

pour l'heure insuffisantes. Une avenue supplémentaire à explorer pourrait être d'initier (ou renouveler) les efforts diplomatiques auprès des États-tiers servant de base arrière aux pirates de Pyongyang, et de collaborer davantage avec certains pays de la région eux aussi visés par ces attaques, comme l'Inde. De fait, tous les pays concernés par ce phénomène partagent au moins un intérêt de long-terme : réduire, de manière visible et crédible, l'attrait du cyber-banditisme d'État dès aujourd'hui, pour éviter que le modèle ne fasse florès demain.

Photo : Roman Harak

•— ••— — • ••— •—• •••

Alexis Rapin

Alexis Rapin (@alexis_rapin) est chercheur en résidence à la Chaire Raoul-Dandurand en études stratégiques et diplomatiques de l'Université du Québec à Montréal. Ses travaux portent notamment sur les transformations de la conflictualité, la cyberdéfense et les opérations d'influence. Il est également membre du comité éditorial du Rubicon.

Comment citer cette publication

Alexis Rapin, « Des bitcoins aux missiles : en Corée du Nord, un cyber-banditisme d'État », *Le Rubicon*, 21 novembre 2024 [https://lerubicon.org/des-bitcoins-aux-missiles-en-coree-du-nord-un-cyber-banditisme-detat/].