Lettre n°39 - juin 2015 - disponible sur omc.ceis.eu

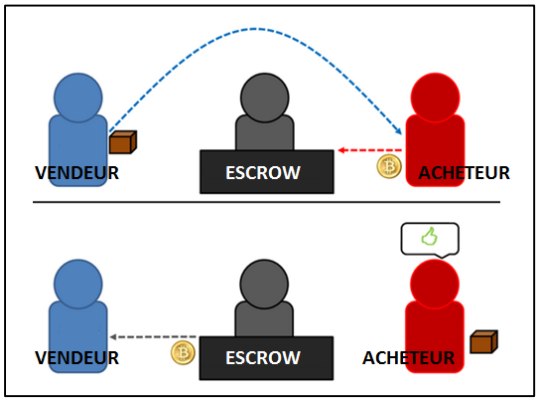
"If somebody would come up to me and say, "Look, Hayden, here's the thing: This Snowden thing is going to be a nightmare for you guys for about two years. And when we get all done with it, what you're going to be required to do is that little 215 program about American telephony metadata -- and by the way, you can still have access to it, but you got to go to the court and get access to it from the companies, rather than keep it to yourself." I go: "And this is it after two years? Cool!" ***Général Michael Hayden, ancien directeur de la NSA***

Table des matières

CYBERCRIMINALITE 2.0 : GUERRE ENTRE LES BLACKMARKETS

Silk Road était un marché noir uniquement accessible via le réseau anonyme Tor et dédié au commerce de tous les types de biens illégaux issus du banditisme classique : stupéfiants, armes ou encore faux papiers. Cette plateforme fut temporairement fermée (quelques semaines) une première fois en 2013 avant d'être définitivement suspendue par le FBI en novembre 2014 au cours de l'opération Onymous qui visait à arrêter les activités illicites d'environ 400 sites.

Silk Road, considéré à ce moment-là comme le plus important « supermarché » du Dark Web, ne proposait pas directement la vente des biens mais mettait en relation acheteurs et vendeurs. Ces derniers concluaient leurs transactions via la crypto-monnaie Bitcoin et l'utilisation du service appelé « escrow » ou plus communément connu sous l'appellation dépôt fiduciaire.



L'escrow est un système de paiement ayant recours à une tierce personne neutre (les administrateurs de Silk Road dans le cas présent) qui veille à ce que le paiement de la transaction soit effectué une fois les conditions remplies (exemple : livraison du produit). Le tiers peut également servir d'arbitrage en cas de différend entre l'acheteur et le vendeur.

La chute de Silk Road vit l'émergence en 2014 et 2015 sur le Dark Web d'un grand nombre de sites souhaitant imiter ce type de commerce. Ainsi, le marché noir Evolution occupa la place de leader, parmi une vingtaine d'acteurs, jusqu'à sa fermeture en mars 2015 suite à un *exit-scam* : les administrateurs du site, qui faisaient office d'escrow, ont fermé leur plateforme empochant les Bitcoins (environ 12 millions USD) placés en dépôt fiduciaire (en attente d'être transmis au vendeur) sur leur plateforme.

Une vingtaine de marchés noirs se sont donc développés à partir du modèle utilisé par Silk Road. Il est possible d'estimer le potentiel du marché actuel en se basant sur le nombre moyen d'annonces proposées par les vendeurs : trois plateformes (AGORA, ALPHABAY et NUCLEUS) se placent en tant que leaders avec une moyenne de 21 550 offres disponibles quotidiennement. Les principales catégories de produits proposés se découpent de la manière suivante :

- Stupéfiants : 60% ;

- Données piratées et produits digitaux (malware, exploit) : 16% ;

- Guides et tutoriaux : 15% ;

- Le reste, 9%, se partage de manière équitable entre : les produits contrefaits, les bijoux et les armes.

Des stratégies concurrentielles classiques

Aujourd'hui, le marché de la vente de produits et services illicites sur le Dark Web est très éclaté et se partage entre une multitude d'acteurs. À l'instar des entreprises classiques opérant de manière légale, les administrateurs qui régissent ces plateformes illicites ont adopté des stratégies concurrentielles et des politiques basées sur l'innovation afin d'augmenter leurs parts de marché.

En raison du potentiel de ce marché mais également du risque élevé de fraude des trois parties impliquées (acheteurs, vendeurs et administrateurs), des mesures de sécurisation et orientées « service client » ont été implémentées par les leaders qui ont rapidement été suivis par le reste des opérateurs du Dark Web. Ainsi, de nombreuses innovations ont été mises en place afin d'attirer de plus en plus de clients et se démarquer de la concurrence :

Avant un achat :

- Enregistrement libre et cooptation : l'accès aux marchés noirs leaders se fait de manière libre lors de l'inscription, ce qui leur permet d'attirer un maximum d'utilisateurs, mais augmente par ailleurs la probabilité d'arnaques. Certaines plateformes ont opté pour un système de cooptation, afin de permettre à une communauté élitiste et se connaissant, de pouvoir échanger en minimisant le risque de fraude. Ce type de système est également utilisé sur les forums lorsque les membres souhaitent communiquer sur des sujets particuliers auprès d'une communauté restreinte et présélectionnée.

- Droit d'entrée et commission : les principaux marchés noirs essayent cependant de contrôler un afflux trop important en imposant un droit d'entrée aux nouveaux vendeurs qui s'élève à une centaine de dollars américains. Les plateformes ayant moins de parts de marché abolissent cette barrière ou instaurent un droit très faible afin d'attirer un maximum de nouveaux utilisateurs. Les administrateurs se rémunèrent via une commission sur les transactions de 4 à 6% contre 2 à 3% pour les leaders qui peuvent se reposer sur une vaste communauté.

Pendant un achat :

- 2FA (code PIN) : le code PIN est renseigné au moment de l'enregistrement sur le black market en complément du pseudonyme et du mot de passe. Il est utilisé comme une méthode de validation secondaire pour se prémunir contre la perte des fonds si le nom d'utilisateur et le mot de passe sont découverts. Il est généralement demandé pour les transferts de fonds vers l'extérieur du marché, ou pour confirmer et finaliser les transactions entre acheteurs et vendeurs.

- Finalize early : certains fournisseurs peuvent exiger que l'achat s'exécute via l'option « Finalize Early », ce système permet de libérer immédiatement l'argent au fournisseur. Le vendeur ne peut cependant pas se faire rembourser si les conditions de la transaction ne sont pas respectées par le vendeur. Cette pratique est utilisée pour limiter le risque de fluctuation du cours du Bitcoin et éviter toute fraude du type *exit-scam* de la part des administrateurs du marché noir. L'option « Finalize Early » est en général attribuée aux vendeurs ayant fait leurs preuves et possédant une excellente notoriété.

- Multi-sig : cette fonctionnalité permet à une transaction d'exiger des approbations multiples indépendantes pour être acceptées. La transaction est sécurisée par les clefs privées de l'acheteur et du vendeur. Ce système permet de limiter au maximum le risque de fraude.

Ces systèmes sont cependant complexes et coûteux à mettre en place. Seuls les puissants marchés noirs ont implémenté ces innovations qui permettent également de minimiser les fraudes.

Après un achat :

- Retour d'expérience : les utilisateurs des marchés noirs ont la possibilité d'échanger entre eux grâce au forum qui est mis à leur disposition. Les rubriques « acheteur » et « vendeur » décrivent des retours d'expérience sur la qualité d'un produit proposé, le délai d'envoi ou encore le professionnalisme appliqué. Dans l'optique d'attirer un maximum d'utilisateurs, le leader des marchés noirs, AGORA, a développé son propre moteur de recherche Grams ainsi qu'une plateforme dédiée à la réputation qui permet d'avoir accès aux fiches profils des meilleurs

vendeurs et des utilisateurs menant des escroqueries.

- Remboursement : les administrateurs des sites ont également un rôle d'arbitre et n'hésitent pas à rembourser un utilisateur qui porterait une réclamation légitime.

Des stratégies concurentielles propres au dark web

Le mois de mai 2015 a été témoin d'un événement marquant au sein de la communauté des utilisateurs des marchés noirs du Dark Web. En effet, ces derniers se sont vivement inquiétés pendant deux semaines de l'indisponibilité des principales plateformes et de l'absence de communication externe des administrateurs de ces sites. La communauté a logiquement supposé qu'il s'agissait d'*exit-scams* (les gérants ferment leur marché noir et partent avec l'ensemble des dépôts fiduciaires, cf. le cas Evolution), mais la réalité est tout autre et témoigne d'une pratique propre au monde du Dark Web. L'administrateur du marché noir NICE GUY a commandité une attaque DDoS massive sur l'ensemble de ses concurrents qui s'est déroulée en plusieurs étapes :

- 1ère étape : l'administrateur de NICE GUY a tout d'abord reçu une demande de rançon (environ 2 000 euros) d'une personne anonyme sous peine de voir son site victime d'une attaque DDoS et donc une indisponibilité de longue durée.

- 2ème étape : l'administrateur a ensuite négocié avec l'attaquant. Il lui proposa un partenariat (200 USD par jour) qui consistait à infliger des attaques DDoS aux huit principaux marchés noirs et ainsi accroître ses revenus et parts de marché.

- 3ème étape : l'administrateur de NICE GUY augmenta son offre en planifiant sur le long terme un *exit-scam* et le partage de plusieurs millions de dollars en cas de réussite.

- 4ème étape : l'attaquant accepta le partenariat et mena pendant deux semaines des campagnes très importantes de DDoS sur l'ensemble des autres marchés noirs ciblés qui furent la plupart du temps inaccessibles.

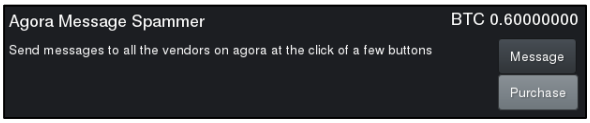
- 5ème étape (en parallèle des quatre premières) : il s'est avéré que l'attaquant avait initialement mené d'autres DDoS contre plusieurs marchés noirs et demandé également des rançons. L'une de ces plateformes (appelée TRD) piégea l'extorqueur. L'administrateur de TRD proposa de négocier la rançon sur un site externe qui était au final un site de phishing destiné à voler les identifiants de l'attaquant. Ces derniers étant également utilisés sur le site NICE GUY, cela permit à l'administrateur de TRD d'avoir accès aux échanges entre l'attaquant et le commanditaire.

- 6ème étape : l'ensemble des échanges fut rendu publique et entraîna une vive réaction de la part de la communauté des marchés noirs qui mena une attaque massive à l'encontre du site NICE GUY.

- 7ème étape : l'ensemble des attaques DDoS s'arrêtèrent quelques jours plus tard.

Cet épisode témoigne de la forte compétition qui existe entre les différents acteurs de la communauté des marchés noirs.

Des actions plus discrètes et visant à détourner les clients d'un marché noir sont également commises de manière régulière. Ainsi, un vendeur réputé de la plateforme TRD (et proche collaborateur de l'administrateur) a récemment découvert une vulnérabilité au sein du système de messagerie interne des marchés noirs AGORA et NICE GUY. L'exploitation de cette vulnérabilité permet d'envoyer un message à l'ensemble des utilisateurs de ces plateformes et par conséquent de faire la promotion de produits ou services d'autres sites du Dark Web :



Conclusion

La compétition entre les marchés noirs du Dark Web se traduit aujourd'hui par une réelle guerre entre les différents acteurs. Ces derniers s'appuient sur des stratégies d'innovation et de relation client afin d'attirer un maximum d'utilisateurs.

Par ailleurs, les différents protagonistes n'hésitent plus à avoir recours à des pratiques cybercriminelles. Alors que la fraude a toujours existé entre acheteurs et vendeurs, les administrateurs s'attaquent de manière directe pour assurer ou gagner des parts de marchés.

COREE DU NORD : DES CAPACITES CYBER EN PROGRESSION

Quoique souvent amplifiée par le prisme américain et sud-coréen, la menace informatique nord-coréenne est réelle. Outre le potentiel technique, les réactions d'un pays acculé, atteint d'une paranoïa collective, peuvent être imprévisibles. Le « quick & dirty » cyber peut faire des dégâts, tandis que la rusticité du pays s'avère être la meilleure défense et un obstacle de poids pour d'éventuelles ripostes. Le degré croissant de sophistication des cyberattaques sur les intérêts sud-coréens et américains ces dernières années laisse en outre présager une amélioration significative des capacités cyber nord-coréennes. Même le bannissement total du pays d'Internet ne saurait supprimer totalement la menace.

A défaut de doctrine cyber connue, on peut au moins gratifier la Corée du Nord d'une certaine constance dans ses orientations stratégiques en matière de cyberespace. Fidèle à sa recherche permanente de l'asymétrie avec ses deux principaux adversaires que sont la Corée du Sud et les Etats-Unis, le pays a développé différentes capacités d'action dans le cyberespace, qu'il s'agisse de lutte informatique, de renseignement ou de guerre psychologique.

De très nombreuses attaques attribuées à la Corée du Nord

La liste des opérations qui lui sont attribuées est ainsi impressionnante. Dès 2004, la Corée du Nord est accusée d'avoir pénétré plusieurs dizaines de réseaux militaires sud-coréens sans fil lors de l'exercice militaire annuel Etats-Unis-Corée du Sud. En octobre 2007, le pays teste une bombe logique, ce qui conduit le Conseil de sécurité de l'ONU à voter une résolution interdisant la vente de certains matériels informatique à la Corée du Nord. En juillet 2009, le pays utilise des réseaux en Autriche, Géorgie, Allemagne, Corée du Sud et même Etats-Unis pour viser la Corée du Sud. En mars 2011, différents médias, banques et opérateurs d'infrastructures sud-coréens sont victime d'une attaque DDOS restée célèbre sous le nom de « 10 days of rain ». En 2013, un virus nommé DarkSeoul est utilisé contre des institutions financières sud-coréennes. Puis c'est une opération d'espionnage massive visant les réseaux militaires sud-coréens et américains et baptisée « Operation Troy » qui est découverte par McAfee.

Dernier fait d'arme attribué à la Corée du Nord : l'attaque visant Sony Picture en décembre 2014. Alors que les studios s'apprêtent à lancer L'interview qui tue, film qui met en scène le dirigeant coréen Kim Jong-Un, l'entreprise fait face à une grave attaque informatique. Revendiquée par un groupe se faisant appelé Guardians of Peace, l'attaque paralyse le système d'information, tandis que des centaines de gigaoctets de fichiers internes sont exfiltrés et publiés sur le web. Sony Picture décide alors de retarder la sortie du film.

Retour sur l'affaire Sony Picture

Aussitôt pointée du doigt par les Etats-Unis, la Corée du Nord dément être à l'origine de l'attaque. Même si le mobile apparait plausible, aucun élément technique n'incrimine de fait le pays. Seule une proximité technique avec le malware utilisé lors de l'opération DarkSeoul en 2013 et quelques termes en coréen dans le code sont relevés. Les pirates, dont les motivations sont peu claires (compensation monétaire, critique de la « cupidité » de Sony Pictures, de la « dangerosité » du film…), démentent en outre être nord-coréens. Si l'origine nord-coréenne de l'attaque est l'une

des hypothèses, **d'autres pistes peuvent donc être esquissées**, parmi lesquelles celle **de l'ancien salarié en délicatesse avec son entreprise** (thèse soutenue par la société américaine Norse) ou bien celle d'un **groupe hacktiviste**, éventuellement sud-coréen, agissant par provocation (hypothèse soulevée par le CSIS américain[1]).

Qualifiée dès le départ de « grave affaire de sécurité nationale » par le porte-parole de la Maison Blanche, l'attaque a échauffé les esprits aux Etats-Unis. Tout en reconnaissant qu'il ne s'agissait pas d'un « acte de guerre », le Président Obama va jusqu'en envisager de remettre la Corée du Nord sur la liste des Etats terroristes. Mais la vraie question est de savoir s'il a autorisé ou non une riposte informatique. La Corée du Nord subit en effet en retour une attaque qui coupe l'unique lien reliant le pays au reste du monde. Une attaque qui n'a pas été revendiquée ni attribuée formellement. Les propos de l'administration américaine déclarant « *examiner une série d'options* », puis les déclarations de Michael McCaul[2], membre du Congrès, indiquant qu'il avait bien eu « ***quelques ripostes informatiques à l'encontre de la Corée du Nord*** » ont cependant laissé planer le doute.

Ce flou arrange d'ailleurs les Etats-Unis qui crédibilisent encore un peu plus **leur capacité à agir et à frapper dans le cyberespace où bon leur semble**. Et ce, alors même que cette opération n'a pas nécessité de gros moyens techniques en raison de la faiblesse des infrastructures nord-coréennes et n'a eu qu'un impact très symbolique du fait du très faible nombre de nord-coréens connectés au réseau mondial.

L'attribution de toutes ces opérations à la Corée du Nord est bien sûr fragile. Les liens qui relient ces opérations à Pyongyang sont parfois tenus : des similarités techniques dans les malware, des caractères coréens dans le code et beaucoup plus rarement des adresses IP nord-coréennes. Et pour cause : avec leur 1024 adresses IP et leur lien unique vers l'extérieur, les infrastructures nord-coréennes ne permettent pas de lancer des opérations d'envergure. Mais d'autres éléments caractéristiques peuvent être identifiés[3] : les dates des opérations (correspondant généralement à l'anniversaire du déclenchement de la guerre de Corée ou au lancement de l'exercice militaire annuel réunissant la Corée du Sud et les Etats-Unis), la nature des cibles, la continuité dans le temps, l'intégration dans les malware d'une fonction de désactivation des logiciels de sécurité de la société sud-coréenne AhnLab, l'utilisation répétée des mêmes types de malware (dropper, wiper et Remote Access Trojan ou RAT).

Autre enseignement : alors que la plupart de ces opérations ne requièrent pas des capacités très sophistiquées, certaines actions sortent du lot, à l'image de l'attaque visant Sony Picture qui a réussi à leurrer tous les systèmes de sécurité de l'entreprise. Cela démontre que **les capacités offensives nord-coréennes ont progressé en quelques années**. Selon Kim Heung-Kwang[4], professeur d'informatique ayant fui la Corée du Nord en 2004, le pays travaillerait aussi à

[1] http://csis.org/publication/sony-and-north-korea-making-case

[2] http://8e-etage.fr/2015/03/18/membre-du-congres-avoue-demi-mot-le-role-des-usa-dans-la-coupure-geante-dinternet-en-coree-du-nord/

[3] https://h30499.www3.hp.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf

[4] http://uk.businessinsider.com/north-korean-defector-professor-kim-heung-kwang-hackers-claim-destroy-city-bureau-21-2015-5?r=US

l'élaboration d'une variante de Stuxnet. Difficile d'établir un lien entre les deux éléments, mais on se souvient que début 2015, la Corée du Sud avait reproché à son voisin de mener des attaques contre ses centrales hydroélectriques et nucléaires.

Une organisation très structurée

Au plan pratique, cette capacité repose sur une organisation associant le Ministère de la défense et le Parti des travailleurs.

Le ministère de la défense abriterait ainsi 3 unités en charge des opérations cyber :

- Le bureau 91, en réalité l'état-major des opérations cyber ;

- L'unité 121, en charge des opérations offensives, **notamment depuis l'un de ses bureaux satellites basé à Shenyang, du côté chinois de la frontière**. Difficile de se faire une idée précise du nombre de « cyber warriors », au vu de l'inflation des chiffres avancés. Les autorités sud-coréennes évoquent aujourd'hui 6 000 personnes ;

- Le lab 110, responsable des aspects techniques et du développement de malware comme DarkSeoul.

Le Parti des travailleurs comprendrait de son côté :

- L'unité 35, en charge de l'entrainement ;

- L'unité 204, responsable des opérations de guerre psychologique et du renseignement cyber. Le pays a institutionnalisé **un *trolling* permanent des messages sud-coréens** sur les forums et médias sociaux grâce à 200 agents ;

- Le bureau 225, qui entraine les agents destinés à partir en Corée du Sud, parfois avec un « bagage » cyber[5].

Au-delà de ces structures apparaissent plusieurs groupes de pirates contrôlés par le régime ou servant de marques pour revendiquer les différentes actions menées. Il s'agit par exemple des groupes Kimsukyang, isOne (qui a revendiqué l'attaque de juin 2012 contre le journal sud-coréen JoongAng Ilbo), WhoIs Team, DarkSeoul (qui utilise le malware du même nom), New Romantic Cyber Army Team. Le pays peut également compter sur le réseau extérieur que forme la diaspora nord-coréenne et notamment l'association Chongryon qui rassemble les nombreux nord-coréens vivant au Japon et interviendrait en soutien, tant en matière de renseignement que d'action, aux opérations nord-coréennes.

A la capacité informatique s'ajoute enfin **une capacité de guerre électronique reconnue**. Le pays a ainsi brouillé le signal GPS pendant un exercice militaire Etats-Unis-Corée du Sud en mars 2011. Des avions de ligne rapportent aussi régulièrement des brouillages de signaux GPS lors de l'approche d'Incheon, l'aéroport de Seoul. Des rapports militaires américains font en outre état d'une capacité IEM (arme à impulsion électromagnétique), développée à partir de technologies fournies par la Russie.

Un faible potentiel industriel

Ces capacités restent cependant entravées par le faible potentiel industriel nord-coréen dans le domaine IT. Malgré les incantations de Kim Jong Il qui avait prophétisé que la personne sans

[5] http://www.pcworld.com/article/2861692/what-we-know-about-north-koreas-cyberarmy.html

ordinateur était l'un des trois idiots du 21ème siècle (les autres étant les fumeurs et les ignorants en matière de musique…), **la base industrielle et technologique apparait extrêmement faible**. Le complexe inter-coréen Kaesong qui fait travailler 54 000 travailleurs nord-coréens au profit d'entreprises du Sud travaille ainsi essentiellement dans le secteur manufacturier (habits, chaussures, montres…). Seule concession à l'ère numérique : le régime a décidé d'y implanter un Business center comprenant 20 ordinateurs connectés… Par ailleurs, l'outsourcing IT au profit de sociétés sud-coréennes et de quelques acteurs occidentaux qui s'était développé dans les années 2000 semble avoir fait long feu. La R&D est donc concentrée essentiellement au sein d'institutions comme le Korean Computer Center qui a par exemple développé, sur une base Linux, le système d'exploitation nord-coréen Red Star, et sur des universités, dont certaines excellent dans le domaine des mathématiques.

Source : © Reuters – KCNA

Ce faible potentiel industriel va de pair avec le **retard des infrastructures IT nord-coréennes**. Avec seulement quelques milliers de privilégiés connectés à Internet et des taux d'équipement extrêmement faibles, la Corée du Nord est le pays le moins connecté du monde. L'accès à internet reste limité à la nomenklatura et aux touristes étrangers dans l'unique datacenter de Pyongyang ou via le réseau 3G proposé par Koryolink. Une seule liaison relie ensuite le pays au réseau mondial via l'opérateur chinois China Netcom. Même s'il est donc théoriquement possible que le pays contrôle des botnets extérieurs grâce à des serveurs de Control & Command locaux, il semble que les attaques soient systématiquement lancées depuis l'étranger, notamment depuis la Chine. L'intranet nord-coréen (Kwangmyong) est quant à lui totalement coupé du monde extérieur et propose à la population locale quelques rares sites parmi lesquels un site marchand (Okryu) récemment lancé avec un système de carte de e-money.

Focus sur les infrastructures IT nord-coréennes

- Un seul Autonomous System.

- 1024 adresses IP (contre 112 millions en Corée du Sud). A noter que certaines adresses IP nord-coréennes font régulièrement l'objet de détournements BGP par des sites de partage (comme thepiratebay en 2013).

- 17 sites web « externes » distincts sur l'ensemble des adresses IP.

- Deux serveurs mail : mail.star.edu.kp et mail.silibank.net.kp.

- 2,4 millions de téléphones mobiles (pour une population de 24 millions).

- Un seul réseau 3G accessible que dans certaines zones urbaines proposé par l'opérateur Cheo Technology sous la marque Koryolink (joint-venture entre l'opérateur égyptien Orascom et Korean Post and Telecommunications Corp).

- Un seul fournisseur d'accès, Star, joint-venture entre Korean Post and Telecommunications Corp et la société thaïlandaise Loxley Pacific. Le FAI est également chargé de l'allocation des adresses IP.

- La connectivité internationale terrestre est assurée depuis 2010 par la Chine et la société

China Netcom. L'AS coréen est en effet uniquement relié à l'AS 1239 de China Netcom.

- Quelques sites internet en .kp, manifestement hébergés localement, sont difficilement accessibles depuis le reste du monde. Exemples : le site de l'université Kim Il Sung : http://www.ryongnamsan.edu.kp/univ/index, celui de l'agence Maritime http://www.ma.gov.kp/ ou celui de l'agence touristique DPRK Today (http://www.dprktoday.com/index.php)[6].

Un isolement fragilisé

Cet isolement est clairement dans les gènes du régime. L'idéologie officielle nord-coréenne considère que le pays est assiégé et doit se défendre de toutes les agressions extérieures. Ne pas être connecté au réseau mondial, c'est donc d'abord protéger sa population des influences néfastes du monde extérieur. Tout ce qui viendrait remettre en cause l'image d'un pays fort et d'un leader charismatique est banni. **Cette position semble pourtant de plus en plus difficile à tenir.** Musiques et films passent facilement la frontière chinoise, au point que le régime a dû récemment se fendre d'une note demandant aux étrangers résident à Pyongyang de ne pas partager localement des supports média pour éviter tout « contenu indésirable »[7]. Instagram a également fait l'objet de blocages ponctuels depuis la Corée du Nord, sans doute pour éviter la transmission en temps réel de photos à l'extérieur. A l'ère des communications instantanées, les touristes étrangers, autorisés à se connecter au réseau 3G local, constituent en effet des maillons faibles. Preuve en est l'incendie spectaculaire dont a été victime un grand hôtel de Pyongyang le 11 juin dernier et dont les photos se sont retrouvées sur Instagram alors que la presse locale avait tu l'épisode. Autre exemple instructif : les très nombreuses photos du photo-reporter David Guttenfelder[8].

Ce retard infrastructurel résulte aussi de la situation économique catastrophique du pays et des sanctions internationales qui interdisent l'exportation en Corée du Nord de nombreuses technologies. Faute de capacités de production locale en matière de hardware informatique, le pays ne peut donc que **compter que sur ses liens avec la Chine et la Russie**, avec laquelle les liens se sont renforcés depuis 2014, pour s'approvisionner tant bien que mal. La Central Scientific and Technological Information Agency, en charge de l'intranet national Kwangmyong, s'appuie ainsi fréquemment sur des expertises russes. Le pays aurait aussi envoyé des experts se former en Russie. Même chose du côté de la Chine qui fournit la connectivité et héberge manifestement certaines activités clandestines nord-coréennes. La Corée du Nord a enfin traditionnellement des liens avec l'Iran dans le domaine de l'armement conventionnel, coopération étendue au domaine cyber depuis la signature d'un traité entre les deux pays en 2012. Destiné à combattre « les ennemis communs » dans le cyberespace, ce traité prévoit, pour sa partie visible, des coopérations en matière de recherche et des échanges d'étudiants.

Facteur aggravant, les capacités de production et de distribution électrique du pays sont hors d'âge, ce qui entraine **de très nombreuses coupures électriques**. Difficile dans ces conditions de mettre en place et d'exploiter des infrastructures informatiques performantes.

[6] http://www.dailymail.co.uk/news/article-2858028/A-place-wind-North-Korea-launches-new-tourism-website-complete-pictures-smiling-children-ski-resort-missiles.html

[7] http://www.torontosun.com/2015/06/26/north-korea-to-foreigners-dont-bring-in-porn

[8] https://instagram.com/dguttenfelder/

Un isolement ambivalent

La faiblesse des infrastructures nord-coréennes et l'isolement du pays apparaissent finalement ambivalents. D'un côté, ils entravent le développement numérique du pays et obèrent ses capacités d'action dans le cyberespace. **De l'autre, ils protègent le pays des attaques informatiques**. La cyber attaque qui a visé la Corée du Nord quelque jours après l'affaire Sony Pictures et coupé le pays du reste du monde n'a ainsi eu qu'un impact très limité. **Une opération Stuxnet bis** visant les centrifugeuses du programme nucléaire nord-coréen (identiques aux centrifugeuses iraniennes) menée par les Etats-Unis aurait même été montée sans succès en 2010[9]. L'isolement du pays et sa faible connectivité rendent en outre particulièrement difficile l'implantation de mouvements de dissidence ou d'hacktivisme anti-régime. En témoigne le **hackaton organisé par la Human Right Foundation** à New York en août 2014 et dont l'objectif était de trouver de nouveaux moyens d'exfiltrer des informations du pays.

[9] http://www.reuters.com/article/2015/05/29/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la Défense et des Anciens combattants
Direction Générale des Relations Internationales et de la Stratégie
14 rue Saint-Dominique - 75700 – Paris SP 07

CEIS
280 Boulevard Saint-Germain - 75007 - Paris
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com