Corée du Nord, cybersécurité et cyberdéfense

Daniel Ventre, Titulaire de la Chaire Cybersécurité & Cyberdéfense

Mars 2016. Article III-24

Le 6 mars 2016, la Corée du Nord menaçait les Etats-Unis et la Corée du Sud de frappes nucléaires aveugles, si les grandes manœuvres militaires conjointes programmées pour le 7 mars par ces deux pays étaient réalisées. Les tensions internationales de ces derniers mois avec Pyongyang, après ses annonces de tests nucléaires et d'essais de missiles, se sont traduites, entre autres, par une résolution de l'ONU et le vote de mesures par la chambre des représentants aux Etats-Unis. Cette nouvelle phase de tension s'inscrit dans le prolongement de plusieurs décennies d'un conflit inachevé entre les deux Corées. La montée en puissance militaire de la Corée du Nord a pour corollaire un sentiment d'insécurité accru chez ses voisins, incité à renforcer leurs développements capacités en matière de sécurité et de défense. La menace n'est pas uniquement régionale : avec l'augmentation de la portée des missiles, la Corée du Nord pourrait frapper les Etats-Unis, affirme-t-elle ; et par le biais des cyberattaques, son périmètre d'attaque est planétaire. Dans ce contexte de tensions élevées, le cyberespace est au fil des années devenu un espace où l'affrontement se prolonge. On peut alors s'interroger sur le rôle que joue le cyberespace dans ce conflit permanent : contribue-t-il à envenimer la situation ou au contraire à la pacifier?

1 – L'actualité cyber de la Corée du Nord

Ces dernières années la Corée du Nord a fait l'objet de multiples accusations de cyberattaques. Les incidents entre les deux Corées constituent une partie essentielle des actes dénoncés, mais concernent également le Japon, les Etats-Unis et nombre d'autres nations. Voici un tableau succinct des cyberattaques impliquant la Corée du Nord, en qualité de responsable ou de cible.

La Corée du Sud accuse la Corée du Nord…	
	En 2013, paralysie des réseaux des entreprises des médias (broadcasting) sud-coréennes et des banques
	En 2014, attaque contre Korea Hydro & Nuclear Power Co. attribuée à la Corée du Nord.

	Fin janvier 2016, le gouvernement de Séoul affirme que le pays a été attaqué par le Nord, mais se refuse à dire précisément quand, quelles cibles ont été touchées, la portée des impacts.
	Les services de renseignement sud-coréens accusent Pyongyang d'avoir espionné en février et mars 2016 les téléphones portables de personnels de ses ministères (dérobant historiques des appels, textes, et interceptant des appels vocaux) (Mu-Huyn, 2016)[1]
La Corée du Nord accuse la Corée du Sud…	
	La Corée du Nord accuse la Corée du Sud et les Etats-Unis de cyberattaques persistantes et intensives[2]
Les Etats-Unis accusent la Corée du Nord…	
	le 19 décembre 2014, les Etats-Unis attribuent à la Corée du Nord les attaques subies par Sony Pictures en novembre de la même année ; le 20 décembre la Corée du Nord demande une enquête conjointe avec les Etats-Unis. Quelques jours plus tard les Etats-Unis publieront la liste des organisations et individus coréens responsables.
	En juillet 2015 la bourse de New-York doit interrompre son fonctionnement. La Corée du Nord aurait revendiqué être à l'origine de cette perturbation par cyberattaques.

Tableau : Quelques cyberattaques impliquant la Corée du Nord

2 - Discours sur la cybermenace nord-coréenne

Le CSIS (Center for Strategic & International Studies) a publié en décembre 2015 un rapport sur les cyberopérations nord-coréennes (Jun, LaFoy, Sohn, 2015)[3]. Le rapport revient sur les conditions du contexte stratégique (la Corée du Nord opte pour une confrontation asymétrique et des opérations irréguières pour contrer la puissance militaire conventionnelle des Etats-Unis et de la Corée du Sud) dans lequel s'insère la cyberstratégie nord-coréenne (qui considère les cyber-capacités comme des instruments du conflit asymétrique, permettant en temps de paix de maintenir un status quo avec

[1] MU-HYUN C. (2016), "South Korea Claims North hacked government official's smartphones", *ZDNet*, 8 février, http://www.zdnet.com/article/south-korea-claims-north-hacked-government-officials-smartphones/?tag=nl.e305&s_cid=e305&ttag=e305&ftag=TRE21e7bbc

[2] AFP (2013)"North Korea Cyber Attacks: Pyongyang accuses South, U.S. of 'persistent and intensive' cyberattack", 15 mars, http://www.huffingtonpost.com/2013/03/15/north-korea-cyber-attacks_n_2881767.html

[3] JUN J., LAFOY S., SOHN E. (2015), "North Korea's Cyber Operations. Strategy and Responses", *Center for Strategic & International Studies*, Washington D.C., décembre, 110 pages, https://csis.org/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf

faibles risques de représailles, et en temps de paix permettant d'atteindre les systèmes C4ISR ennemis).
Le rapport décrit ensuite l'organisation des acteurs de cette cyberstratégie (le bureau central du renseignement ; l'Etat-Major ; une base technologique industrielle à la fois logicielle et matérielle).
Le rapport formule enfin un certain nombre de recommandations pour la politique américaine (préparer des réponses graduées contre les responsables ; limiter la liberté d'action nord-coréenne dans le cyberespace ; identifier les vulnérabilités du cyberespace nord-coréen ; adapter le niveau de réponse à la gravité, notamment en développant un cadre juridique national et en promouvant une évolution du système juridique international) et celle de rapprochement avec la Corée du Sud (partage d'information, dialogue, élargir la confiance et la coopération dans la région…)

Plusieurs thèmes concentrent les débats sur les cyber-capacités nord-coréennes, tant dans la presse que dans des rapports d'experts, voire des études académiques.
La cybermenace nord-coréenne se traduit par des intrusions et tentatives d'intrusion dans les réseaux et serveurs d'entreprises et gouvernements étrangers. 5000 à 6000 hackers militaires constitueraient les cyber-forces du pays. L'idée d'utiliser les ordinateurs pour attaquer les ennemis et le début de construction de capacités cyberoffensives remonteraient aux années 1990 (donc au même moment que dans le reste du monde), selon Kim Heung-kwang et Jang Sae-yul, deux transfuges nord-coréens[4]. Après quelques années de formation notamment à l'étranger, l'armée nord-coréenne ouvrit le Bureau 121 (unité de cyberdéfense), en 1998. Selon le Livre Blanc du Ministère de la Défense sud-coréen, l'armée du nord compterait entre 5000 et 6000 agents au sein de ses cyber-unités qui, selon un rapport du NKIS, think tank basé à Séoul, seraient constituées ou en construction depuis 16 ans. L'histoire des unités militaires cyber nord-coréenne est donc assez imprécise, sa genèse remontant pour les uns au début des années 1990, pour d'autre des années 2000. Les commentaires convergent, semble-t-il, vers un constat: la cyberdéfense nord-coréenne n'est pas balbutiante.

L'internet nord-coréen n'existe pas	Il est dans un tel état minimaliste qu'il est exagéré de qualifier le réseau nord-coréen d' « internet »
La Corée du Nord ne peut pas être victime de cyber-attaques	Le pays reste à l'écart des cybermenaces, ne disposant pas d'un véritable internet (Peterson, 2015)[5]
La Corée du Nord est accusée de cyberattaques (contre la Corée du Sud, le Japon, …)	L'état minimaliste, rudimentaire du réseau nord-coréen lui fournirait toutefois assez de ressources pour mener des cyberattaques (ayant ainsi le pouvoir d'attaquer sans être pour autant trop vulnérable, car peu dépendant du cyberespace).
La Corée du Nord dément les accusations portées à son encontre	Les Etats ne reconnaissent pas les cyberattaques dont on les accuse. La Corée du Nord ne déroge pas à ce principe[6].
La Corée du Nord accuse	La Corée du Nord accuse les Etats-Unis de

[4] Cités dans : SANGER D.E., FACKLER M. (2015), "NSA breached north Korean networks before Sony attack, Officials say", The New York Times, 18 janvier, http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0
[5] PETERSON A. (2015), "A U.S. cyberattack on North Korea failed because North Korea has basically no Internet", *The Washington Post*, 1° juin, https://www.washingtonpost.com/news/the-switch/wp/2015/06/01/a-u-s-cyberattack-on-north-korea-failed-because-north-korea-has-basically-no-internet/
[6] http://www.huffingtonpost.com/huff-wires/20130412/as-koreas-cyberattack/

	cyberattaques contre son réseau internet (perturbations du réseau le 22 décembre 2014)
La Corée du Nord méfiante vis-à-vis de toute forme d'introduction de technologies de télécommunication étrangères, débordant ses capacités de contrôle sur les communications dans le pays.	La Corée du Nord veut juguler la diffusion incontrôlée des téléphones portables chinois passés dans le pays en contrebande[7]. Les autorités surveillent les citoyens. Répression des usages jugés illégaux. Communiquer avec l'étranger est un crime.
La Corée du Nord dispose de capacités militaires cyberoffensives et défensives	Le réel niveau de ces capacités demeure difficilement appréciable. Mais il en est de même de tous les pays qui affichent de telles capacités.
Les capacités de cyberdéfense nord-coréennes ne sont pas récentes	La Corée du Nord a pris le train du développement de capacités de cyberdéfense dès le début des années 1990. Elle n'accuserait donc pas de retard dans le domaine.
Les cyberattaques nord-coréennes peuvent être menées de l'étranger	La Corée du Nord peut-elle compter sur des alliances, des soutiens de pays étrangers pour l'aider à monter les opérations de cyberattaques ?

Tableau : Quelques thèmes clefs qui alimentent les débats sur la cybersécurité/défense et l'internet nord-coréen

3 – Les conséquences de la cyber-menace nord-coréenne

3.1. Un ensemble de mesures prises contre la cybermenace nord-coréenne

Les sanctions prises par tout un ensemble d'acteurs de la scène internationale concernent plusieurs domaines : la défense (armes nucléaires, armes de destruction massive…) ; le commerce international (contrôle des exportations d'armes vers et à partir de la Corée du Nord ; secteur nucléaire, mais aussi pêche, industrie, etc.) ; le domaine financier ; la culture (échanges interdits par exemple entre les deux Corées) ; l'accueil de ressortissants nord-coréens dans pays étrangers… Début 2016 l'ONU a voté une nouvelle résolution (n°2270) contre la Corée du Nord (s'ajoutant aux résolutions 1718 (de 2006) ; 1874 (de 2009) ; 2087 et 2094 (de 2013)[8] ; la Corée du Sud a imposé la fermeture du complexe de Kaesong ; le Japon a renforcé les mesures existantes à l'encontre de la Corée du Nord ; l'Union Européenne s'appuie quant à elle sur l'ensemble des décisions du Conseil en vigueur depuis 2013[9].
Des mesures ont également été prises en matière de cybersécurité ces derniers mois.

[7] http://www.lefigaro.fr/international/2016/03/09/01003-20160309ARTFIG00385-kim-jong-un-en-croisade-contre-les-telephones-portables-chinois.php#xtor=AL-201

[8] Un résumé de ces résolutions est disponible à l'adresse: https://www.armscontrol.org/factsheets/UN-Security-Council-Resolutions-on-North-Korea

[9] La liste complète des mesures qui s'appliquent à la Corée du Nord (mais aussi à un ensemble d'autres pays) est disponible dans le document de synthèse en ligne à l'adresse http://eeas.europa.eu/cfsp/sanctions/docs/measures_en.pdf

Le 2 janvier 2015 les Etats-Unis ont désigné les responsables des cyberattaques contre Sony[10] (cette attribution aurait été possible grâce aux informations collectées par la NSA[11]) :

- Le bureau central du renseignement (Reconnaissance General Bureau), qui est la principale agence de renseignement du pays
- Le KOMID (Korea Mining Development Trading Corporation), marchand d'armes nord-coréen, exporte biens et équipements pour missiles balistiques et armes conventionnelles
- La Korea Tangun Trading Corporation (qui agit également dans le monde sous d'autres noms: Ryung Seng Trading Corporation, Ryungseng Trading Corporation, Ryungsong Trading Corporation)
- Kil Jong Hun, fonctionnaire du gouvernement nord-coréen (représentant de la KOMID en Namibie)
- Kim Kwang Yon, fonctionnaire du gouvernement nord-coréen (représentant dela KOMID en Afrique)
- Jang Song Chol, représentant de la KOMID en Russie, fonctionnaire du gouvernement nord-coréen, travaille également avec le Soudan
- Yu Kwang Ho, fonctionnaire du gouvernement nord-coréen
- Kim Yong Chol, représentant de la KOMID en Iran et fonctionnaire du gouvernement nord-coréen
- Jang Yong Son, représentant de la KOMID en Iran et fonctionnaire du gouvernement nord-coréen
- Kim Kyu, responsable des affaires étrangères de la KOMID, fonctionnaire du gouvernement nord-coréen
- Ryu Jin, opérant pour la KOMID en Syrie, fonctionnaire du gouvernement nord-coréen
- Kang Ryong, opérant pour la KOMID en Syrie, fonctionnaire du gouvernement nord-coréen
- Kim Kwang Chin, représentant de la Korea Tangun Trading Corporation à Shenyang (Chine), et lui aussi fonctionnaire du gouvernement nord-coréen

On retrouve deux types d'accusés dans ce dossier : des organismes et des individus (des informations plus précises sur leur identité, telles que dates de naissance, numéros de passeport, sont disponibles sur le site du Département au Trésor)[12]. Cette méthode de mise en accusation individuelle rappelle la procédure lancée par les Etats-Unis en mai 2014 contre 5 militaires chinois accusés de cyberespionnage.

La succession d'incidents de nature cyber, attribués à la Corée du Nord notamment (mais pas uniquement) convainc les autorités de Séoul de la nécessité de renforcer son organisation de cybersécurité. Les autorités créent la fonction de responsable de la cybersécurité et nomment un professeur d'université de la Korea University au poste de conseiller du gouvernement sur ces questions.

---

[10] "Treasury imposes sanctions against the government of the Democratic People's Republic of Korea", *U.S. Department of the Treasury,* février 2015, https://www.treasury.gov/press-center/press-releases/Pages/jl9733.aspx

[11] Cette dernière se serait d'ailleurs introduite dans les réseaux nord-coréens bien avant les attaques contre Sony.

- WILLAMS M. (2015), « NSA had access to North Korean computer network, says report", North Korea Tech, 19 janvier, http://www.northkoreatech.org/2015/01/19/nsa-had-access-to-north-korean-computer-network-says-report/
- SANGER D.E., FACKLER M. (2015), "NSA breached north Korean networks before Sony attack, Officials say", The New York Times, 18 janvier, http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0

[12] Informations détaillées : https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20150102.aspx

En février 2016, la Chambre des Représentants des Etats-Unis a voté une nouvelle loi de sanctions contre la Corée du Nord[13], qui prévoit des mesures dans plusieurs domaines, dont la cybersécurité (WERTZ, 2016) [14]. Le texte rappelle que la Corée du Nord a été impliquée à plusieurs reprises dans des activités illicites, portant notamment atteinte à la cybersécurité des Etats-Unis (le texte mentionne les cyberattaques contre Sony) ou à celle de la Corée du Sud (le texte mentionne les attaques « Dark Seoul », désignant les cyberattaques du 20 mars 2013 ayant touché les infrastructures des médias et de la finance sud-coréenne). Les Etats-Unis appliqueront des sanctions à l'encontre des personnes impliquées dans ces cyber-opérations agressives (le document parle même des personnes et institutions impliquées dans le cyberterrorisme et le développement de capacités de cyberguerre), et souhaitent que les pays membres des Nation Unies s'engagent dans la même voie de sanctions.

3.2. Une coopération internationale qui s'organise contre la menace nord-coréenne

Sur fond de cybersécurité, les relations internationales se développent : politique, militaire, commerciale notamment. Microsoft a créé en Corée un centre de cybersécurité. Sir le plan politique, Corée du Sud et Etats-Unis ont annoncé vouloir renforcer leur coordination en matière de cybersécurité (octobre 2015). Les Etats-Unis sont à la recherche d'alliés dans la lutte contre la Corée du Nord et la cybersécurité est devenue un motif de rapprochement des Etats. Elle est aussi devenue un vecteur du renforcement de la présence nord-américaine dans la région. Concrètement, que comportent ces coopérations de cybersécurité ? Quelle est l'efficacité réelle de ces coopérations, lorsqu'elles ne se résument pas à de simples déclarations d'intentions ?

Conclusion

Les avis demeurent très partagés, concernant le degré de dangerosité des pratiques de cyberdéfense de la Corée du Nord et de ses capacités dans le domaine. Que représentent les cybercapacités militaires dans le système de défense nord-coréen ? Selon le transfuge Kim Heung-kwang (d'après des déclarations faites à la BBC), 10 à 20% du budget de la défense nord-coréenne serait dédié aux opérations en ligne. Pour les uns la Corée du Nord est une cyber-menace majeure, pour d'autres au contraire une menace qui doit être relativisée (Lee, Kwek, 2015)[15].

La Corée du Nord est-elle si agressive dans le cyberespace que ne le laissent entendre les déclarations sud-coréennes ou nord-américaines ? La liste[16] des incidents attribués à la Corée du Nord, que publie le CSIS dans son rapport de 2015, est bien courte : elle n'en relève que 9 depuis 2009.

[13] Document integral: https://www.congress.gov/bill/114th-congress/house-bill/757/text
[14] WERTZ D. (2016), Summary of the North Korea Sanctions and Policy Enhancement Act of 2016, Washington, février, 7 pages, http://www.ncnk.org/resources/publications/HR757_Summary_Final.pdf
[15] LEE D., KWEK N., « North Korean hackers 'could kill', warns key defector", BBC News, 29 mai, http://www.bbc.com/news/technology-32925495
[16] https://csis.org/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf