Avis relatif à la cybermenace de la RPDC

Date d'émission : 15 avril 2020

Titre : Directives concernant la cybermenace nord-coréenne

Le département d'État, le département du Trésor, le département de la sécurité du territoire et le Federal Bureau of Investigation (FBI) des États-Unis émettent le présent avis, lequel constitue une ressource générale concernant la cybermenace nord-coréenne pour la communauté internationale, les défenseurs de réseaux et le grand public. Y figurent une description des cybermenaces provenant de la Corée du Nord – officiellement la République populaire démocratique de Corée (RPDC) – et des recommandations sur les mesures à prendre pour atténuer ces menaces. Il contient en particulier à l'annexe 1 une liste des ressources du gouvernement des États-Unis relatives aux cybermenaces de la RPDC et à l'annexe 2 un hyperlien vers les rapports du Groupe d'experts du Comité des sanctions pour la RPDC mis en place par la résolution 1718 du Conseil de sécurité des Nations Unies.

Les cyberactivités malveillantes de la RPDC visent les États-Unis et l'ensemble de la communauté internationale et font peser en particulier des menaces significatives sur l'intégrité et la stabilité du système financier international. Sous la pression de robustes sanctions imposées par les États-Unis et les Nations Unies, la RPDC a de plus en plus recours à des activités illicites – notamment à des cyberactivités criminelles – en vue de se procurer des recettes pour financer ses programmes d'armes de destruction de masse et de missiles balistiques. Les États-Unis s'inquiètent profondément, en particulier, des cyberactivités malveillantes de la RPDC, que les autorités américaines dénomment HIDDEN COBRA (COBRA CACHÉ). La RPDC est en mesure de mener des cyberactivités perturbatrices ou destructrices affectant l'infrastructure critique des États-Unis. Elle emploie également ses cybercapacités pour voler des avoirs d'institutions financières et se livre systématiquement à des cyberactivités perturbatrices et malveillantes qui sont absolument incompatibles avec ce qui, selon le consensus international croissant, constitue un comportement responsable des États dans le cyberespace.

Les États-Unis œuvrent étroitement avec les pays animés du même esprit pour attirer l'attention sur le comportement perturbateur, destructeur ou, d'autre manière, déstabilisateur de la RPDC dans le cyberspace. C'est ainsi, par exemple, qu'en décembre 2017, l'Australie, le Canada, les États-Unis, la Nouvelle-Zélande et le Royaume-Uni ont attribué publiquement l'attaque au logiciel de rançon WannaCry à la RPDC et ont dénoncé les cyberactivités nuisibles et irresponsables de celle-ci. Le Danemark et le Japon ont émis des déclarations de soutien en

faveur de la dénonciation conjointe de ladite attaque, qui a affecté des centaines de milliers d'ordinateurs de par le monde en mai 2017.

Il est d'une importance vitale que la communauté internationale, les défenseurs de réseaux et le public restent vigilants et œuvrent de concert pour réduire la cybermenace présentée par la Corée du Nord.

Cyberactivités malveillantes de la RPDC ciblant le secteur financier

De nombreux cyber-acteurs relèvent d'entités désignées par les Nations Unies et les États-Unis, telles que le Bureau général de reconnaissance [de la RPDC]. Les cyber-acteurs nord-coréens financés par l'État sont principalement des pirates informatiques, des cryptologues et des concepteurs de logiciel qui se livrent à de l'espionnage, commettent, par des moyens informatiques, des vols ciblant des institutions financières et des plateformes d'échange de monnaie numérique et mènent des opérations à motivation politiques visant des entreprises de médias étrangères. Ils conçoivent et déploient de par le monde une large gamme d'outils maliciels pour mener ces activités et se montrent de plus en plus élaborés. Au nombre des tactiques communément employées par les cyber-acteurs parrainés par la RPDC pour se procurer des revenus illicites figurent notamment (sans s'y limiter) :

Vol de fonds et blanchiment d'argent. Le rapport de mi-mandat 2019 du Groupe d'experts du Comité du Conseil de sécurité des Nations Unies mis en place par la résolution 1718 dudit Conseil (rapport de mi-mandat 2019 du Groupe d'experts) signale que la RPDC est de plus en plus capable de se procurer des recettes en dépit des sanctions imposées par le Conseil de sécurité des Nations Unies en menant des cyberactivités malveillantes pour subtiliser des fonds à des institutions financières au moyen de tactiques et d'outils de plus en plus élaborés. Le rapport de mi-mandat 2019 du Groupe d'experts note que, dans certains cas, ces cyberactivités malveillantes ont également porté sur le blanchiment de capitaux par le recours à de multiples juridictions. Le Groupe d'experts mentionne dans son rapport de mi-mandat 2019 qu'il enquête sur des dizaines de vols informatiques dont la RPDC était soupçonnée et qu'en date de la fin 2019, celle-ci avait tenté de s'approprier jusqu'à 2 milliards de dollars par le biais de telles cyberactivités illicites. Les allégations émises dans une demande de saisie du département de la Justice de mars 2020 sont en cohérence avec certains des constats du Groupe d'experts. La demande de confiscation allègue en particulier que des cyber-acteurs nord-coréens ont fait usage de l'infrastructure nord-coréenne au service de leur conspiration ayant pour objet de pirater des plateformes d'échange de monnaie numérique, de s'approprier des centaines de millions de dollars en monnaie numérique et de blanchir les fonds.

Campagnes d'extorsion. Des cyber-acteurs de la RPDC ont également mené des campagnes d'extorsion à l'encontre d'entités de pays tiers en compromettant le réseau de l'entité visée et en menaçant de fermer ce réseau s'il ne leur était pas versé une rançon. Dans certains cas, des cyber-acteurs de la RPDC ont exigé de leurs victimes le versement de paiements sous forme d'arrangements de consultation à long terme pour s'assurer que de telles cyberactivités malveillantes ne se reproduisent pas. Des cyber-acteurs de la RPDC ont également été payés pour pirater des sites web et extorquer des cibles pour des tiers clients.

Cryptopiratage. Le Groupe d'experts des Nations Unis note dans son rapport de mi-mandat 2019 qu'il enquête aussi sur l'usage fait par la RPDC du « cryptopiratage », à savoir un stratagème par lequel un ordinateur victime est compromis et ses ressources informatiques sont utilisées pour miner des fonds en monnaie numérique. Le Groupe d'experts a repéré plusieurs incidents où des ordinateurs infectés par un logiciel malveillant de cryptopiratage ont acheminé les fonds ainsi extraits – en grande partie en monnaie numérique à anonymat renforcé (parfois dénommée « monnaie privée ») – vers des serveurs se trouvant en RPDC, notamment à l'Université Kim Il Sung de Pyongyang.

Ces activités mettent en exergue l'usage fait par la RPDC de moyens informatiques pour générer des recettes tout en atténuant l'impact des sanctions et montrent que tout pays peut y être exposé et être exploité par la RPDC. Selon son rapport de mi-mandat 2019, le Groupe d'experts enquête également sur des activités telles que des violations des sanctions du Conseil de sécurité des Nations Unies à l'encontre de la RPDC.

Cyber-opérations attribuées publiquement à la RPDC par le gouvernement des États-Unis

La RPDC a ciblé à de multiples reprises les réseaux gouvernementaux et militaires des États-Unis et d'autres pays, ainsi que des réseaux en rapport avec des entités privées et l'infrastructure critique, pour s'approprier des données et mener des cyberactivités perturbatrices et destructrices. À ce jour, le gouvernement des États-Unis a attribué publiquement les cyber-incidents suivants à des cyber-acteurs et à des co-conspirateurs soutenus par l'État nord-coréen:

- ***Sony Pictures***. En novembre 2014, des cyber-acteurs parrainés par la RPDC auraient lancé une cyber-attaque sur Sony Pictures Entertainment (SPE) en représailles suite à la distribution en 2014 du film « L'interview qui tue ! ». Des cyber-acteurs de la RPDC ont piraté le réseau de SPE pour voler des données confidentielles, ont menacé des dirigeants et des employés de SPE et ont endommagé des milliers d'ordinateurs.

    - Bulletin du FBI sur l'enquête concernant Sony (19 décembre 2014) https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation
    - Plainte pénale du département de la Justice contre un programmeur appuyé par le régime de la Corée du Nord (6 septembre 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***Attaque contre la Banque du Bangladesh***. En février 2016, des cyber-acteurs parrainés par la RPDC auraient tenté de subtiliser au moins un milliard de dollars auprès d'institutions financières de par le monde et auraient volé 81 millions de dollars à la Banque du Bangladesh par le biais de transactions non autorisées sur le réseau de la Société de télécommunications interbancaires mondiales (SWIFT). Selon la plainte déposée, des cyber-acteurs de la RPDC ont accédé aux terminaux informatiques de la Banque du Bangladesh en interface avec le réseau SWIFT après avoir compromis le réseau informatique de la banque au moyen de courriels d'hameçonnage ciblant des employés de la banque. Les cyber-acteurs de la RPDC ont

ensuite envoyé des messages SWIFT frauduleusement authentifiés donnant ordre à la Federal Reserve Bank of New York de virer des fonds du compte de la Banque du Bangladesh auprès de la Federal Reserve sur des comptes contrôlés par les conspirateurs.

  - Plainte pénale du département de la Justice contre un programmeur appuyé par le régime de la Corée du Nord (6 septembre 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***WannaCry 2.0***. Des cyber-acteurs parrainés par la RPDC ont conçu un logiciel rançonneur connu sous le nom de WannaCry 2.0, ainsi que deux versions antérieures de ce logiciel. En mai 2017, le logiciel WannaCry 2.0 a infecté des milliers d'ordinateurs dans des hôpitaux, des établissements d'enseignement, des entreprises et des résidences privées de plus de 150 pays. Le logiciel de rançon WannaCry 2.0 encrypte les données de l'ordinateur infecté et permet aux cyber-acteurs d'exiger le paiement d'une rançon en monnaie numérique Bitcoin [pour les décrypter]. Le département du Trésor a désigné un programmeur informatique nord-coréen en raison de son rôle dans la conspiration WannaCry 2.0 ainsi que dans la cyber-attaque contre Sony Pictures et dans le vol à la Banque Bangladesh ; il a de même été désignée l'organisation pour laquelle il travaillait.

  - Alerte technique du CISA : Indicateurs associés au logiciel de rançon WannaCry (12 mai 2017) https://www.us-cert.gov/ncas/alerts/TA17-132A
  - Point de presse de la Maison-Blanche sur l'attribution du logiciel de rançon WannaCry (19 décembre 2017) https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/
  - Plainte pénale du département de la Justice contre un programmeur appuyé par le régime de la Corée du Nord (6 septembre 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and
  - Communiqué du Trésor imputant de multiples cyberattaques à la Corée du Nord (6 septembre 2018) https://home.treasury.gov/news/press-releases/sm473

- ***Campagne FASTCash.*** Depuis la fin 2016, des cyber-acteurs parrainés par la RPDC ont recours à un système frauduleux de retrait d'espèces à des distributeurs automatiques de billets/guichets automatiques bancaires DAB/GAB, système connu sous le nom de « FASTCash », pour subtiliser des millions de dollars à des DAB/GAB en Asie et en Afrique. Les systèmes FASTCash compromettent à distance les serveurs d'applications de commutation de paiement au sein des banques pour faciliter les transactions frauduleuses. Lors d'un incident en 2017, des cyber-acteurs de la RPDC ont permis le retrait simultané d'espèces dans des DAB/GAB situés dans plus de 30 pays. Lors d'un autre incident survenu en 2018, des cyber-acteurs de la RPDC ont permis de retirer simultanément des espèces de DAB/GAB dans 23 pays.

- Alerte du CISA sur la campagne FASTCash (2 octobre 2018) https://www.us-cert.gov/ncas/alerts/TA18-275A
- Rapport d'analyse de maliciel du CISA : maliciel relatif à FASTCash (2 octobre 2018) https://www.us-cert.gov/ncas/analysis-reports/AR18-275A

- ***Intrusion dans un site de change de crypto-monnaie.*** Ainsi qu'il est décrit dans les allégations énoncées dans une plainte du département de la Justice visant à une saisie réelle, en avril 2018, des cyber-acteurs parrainés par la RPDC ont piraté un site de change de crypto-monnaie et ont subtilisé près de 250 millions de dollars. La plainte précise en outre que les fonds subtilisés ont fait l'objet de blanchiment au moyen de centaines de transactions automatisées en monnaie numérique afin de dissimuler leur origine et d'empêcher les autorités de répression de retrouver les avoirs. Ainsi qu'il est allégué dans la plaine, deux ressortissants chinois auraient procédé ultérieurement à un blanchiment des fonds pour le compte du groupe nord-coréen et reçu environ 91 millions de dollars provenant de comptes contrôlés par la RPDC, ainsi que 9,5 millions de dollars de plus provenant du piratage d'un autre site de change. En mars 2020, le département du Trésor a désigné les deux individus en vertu des dispositions relatives à la cybercriminalité et aux sanctions à l'encontre de la RPDC ; parallèlement, le département de la Justice a annoncé que ces individus avaient précédemment été accusés de blanchiment de capitaux et de transmission non autorisée de fonds et que 113 comptes en monnaie numérique étaient sous le coup d'une saisie.

  - Sanctions du département du Trésor à l'encontre d'individus blanchissant des avoirs en crypto-monnaie pour le Groupe Lazarus (2 mars 2020) https://home.treasury.gov/news/press-releases/sm924
  - Inculpation par le département de la Justice de deux ressortissants chinois accusés de blanchiment de fonds en crypto-monnaie provenant du piratage de sites de change et plainte civile pour saisie (2 mars 2020) https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack

Mesures de parade à la cybermenace de la RPDC

La Corée du Nord cible l'infrastructure informatique au niveau mondial en vue de dégager des recettes pour financer des activités prioritaires du régime au pouvoir, notamment ses programmes d'armes de destruction massive. Nous invitons instamment les autorités gouvernementales, les entités industrielles, la société civile et les particuliers à appliquer toutes les mesures pertinentes énoncées ci-dessous pour se protéger des cybermenaces de la RPDC et pour y parer :

- **Sensibilisation à la cybermenace de la RPDC**. La diffusion d'informations sur la gravité, l'ampleur et la diversité des cyberactivités malveillantes menées par la RPDC aura pour effet d'accroître la sensibilité des secteurs public et privé à ces menaces ainsi que de promouvoir l'adoption et la mise en application de mesures appropriées de prévention et d'atténuation des risques.

- **Partage des informations techniques concernant les cybermenaces de la RPDC**. Le partage des informations au niveau tant national qu'international pour détecter to les cybermenaces de la RPDC et y parer permettra d'accroître la cyber-sécurité des réseaux et des systèmes. Les pratiques optimales devraient faire l'objet d'échanges entre les gouvernements et le secteur privé. En vertu des dispositions de la Loi sur le partage des informations de cybersécurité de 2015 (paragraphes 1501 à 1510 du titre 6 du Code des États-Unis), les entités non fédérales peuvent partager les indicateurs de cybermenace et les mesures défensives concernant HIDDEN COBRA avec des entités fédérales et non fédérales.

- **Mise en application et promotion des pratiques optimales en matière de cyber-sécurité**. L'adoption de mesures, tant techniques que comportementales, de renforcement de la cybersécurité aura pour effet d'accroître la sécurité et la résilience de l'infrastructure cybernétique américaine et mondiale. Les institutions financières, y inclus les entreprises de services monétaires, devraient prendre des mesures indépendantes pour se protéger des cyberactivités malveillantes de la RPDC. Ces mesures peuvent comprendre notamment, sans que l'énumération suivante ait valeur limitative, le partage de renseignements sur les menaces par le canal des organismes gouvernementaux et/ou des entités commerciales et industrielles, la segmentation des réseaux pour minimiser les risques, la tenue régulière de copies de sauvegarde des données, les activités de formation et de sensibilisation sur les tactiques communes d'ingénierie sociale, la mise en application de politiques régissant le partage de l'information et l'accès aux réseaux, et l'élaboration de plans de riposte aux incidents cybernétiques. Le modèle de maturité des capacités en matière de cyber-sécurité (Cybersecurity Capability Maturity Model) du département de l'Énergie et le cadre de cyber-sécurité de l'Institut national des normes et de la technologie (National Institute of Standards and Technology's Cybersecurity Framework) fournissent des conseils sur l'élaboration et l'application de pratiques robustes en matière de cyber-sécurité. Ainsi qu'il est indiqué à l'annexe I, l'Agence de cyber-sécurité et de sécurité de l'infrastructure (Cybersecurity and Infrastructure Security Agency - CISA) offre de vastes ressources, notamment des alertes techniques et des rapports d'analyse de maliciels, pour permettre aux défenseurs de réseaux de repérer et de réduire l'exposition aux cyberactivités malveillantes.

- **Notification des autorités**. Si une organisation soupçonne avoir été victime de cyberactivités malveillantes, émanant de la RPDC ou d'ailleurs, il est essentiel qu'elle en notifie les autorités de répression dans les meilleurs délais. Ceci permet non seulement d'accélérer l'enquête mais peut aussi, dans l'éventualité de la commission d'un crime financier, accroître les chances de recouvrement des avoirs volés.

  Les autorités de répression des États-Unis ont saisi des millions de dollars en monnaie numérique volés par des cyber-acteurs nord-coréens. Les institutions financières de tous types, y inclus les entreprises de services monétaires, sont encouragées à coopérer en amont en accédant aux demandes de renseignements des autorités de répression des États-Unis relatives à ces cybermenaces, et en aval en identifiant les

avoirs confiscables sur réception de demandes de ces autorités ou de décisions de tribunaux des États-Unis et en coopérant avec les autorités de répression des États-Unis pour appuyer la saisie de tels avoirs.

- **Renforcement de la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération (LBC/FT)**. Les pays devraient appliquer promptement et efficacement les normes du Groupe d'action financière (GAFI) sur la LBC/FT. Il s'agit notamment qu'ils veillent à ce que les institutions financières et autres entités couvertes recourent à des mesures d'atténuation des risques alignées sur les normes, les déclarations publiques et les orientations du GAFI. Le GAFI a, en particulier, appelé tous les pays à appliquer des contremesures pour protéger le système financier international des risques de blanchiment de capitaux, de financement du terrorisme et de financement de la prolifération émanant de la RPDC.[1] Il s'agit notamment d'informer toutes les institutions financières et autres entités couvertes de la nécessité d'accorder une attention particulière aux relations d'affaires et aux transactions avec la RPDC, y inclus avec les sociétés et institutions financières de la RPDC et ceux qui agissent pour leur compte. Conformément aux dispositions du paragraphe 33 de la résolution 2270 du Conseil de sécurité des Nations Unies, les États Membres devraient fermer les agences, filiales et bureaux de représentation des banques de la RPDC sis sur leur territoire et mettre fin aux relations de correspondance avec lesdites banques.

  En outre, en juin 2019, le GAFI a amendé ses normes pour exiger que tous les pays réglementent et supervisent les prestataires de services sur actifs numériques, notamment les sites de change de monnaie numérique, et d'atténuer les risques lors de la réalisation d'opérations en monnaie numérique. Les prestataires de services sur actifs numériques doivent surveiller les changements intervenant dans les activités de leurs clients, étant donné que leur entreprise peut être utilisée pour faciliter le blanchiment de capitaux et le financement du terrorisme et de la prolifération. Les États-Unis se préoccupent tout particulièrement des plateformes qui offrent des services anonymes de paiement et de gestion de comptes sans obligations, entre autres, de surveillance des transactions, de déclaration des activités suspectes et de procédures de vigilance à l'égard de la clientèle.

  Les institutions financières des États-Unis, y inclus les prestataires de services sur actifs numériques établis à l'étranger qui mènent leurs activités intégralement ou en grande partie aux États-Unis, et les autres entreprises et personnes couvertes devraient veiller à respecter leurs obligations réglementaires en vertu de la Loi sur le secret bancaire (telle qu'appliquée par l'entremise du Réseau pour la répression des délits financiers (FinCEN) du département du Trésor en vertu du chapitre X du titre 31 du Code des règlements fédéraux). Les institutions financières sont ainsi tenues d'élaborer et d'appliquer des programmes efficaces de lutte contre le blanchiment de capitaux qui sont raisonnablement conçus pour empêcher que les entreprises de

[1] *Le texte complet de l'Appel à l'action du GAFI sur la Corée du Nord est disponible à l'adresse suivante :* https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html.

services monétaires soient utilisées pour favoriser le blanchiment de capitaux et le financement d'activités terroristes, ainsi que de repérer et de signaler les transactions suspectes, notamment celles qui sont menées, effectuées ou facilitées par des moyens informatiques ou les opérations financières illicites concernant des avoirs numériques, dans des déclarations d'activités suspectes transmises au FinCEN.

Coopération internationale. Pour contrecarrer les cyberactivités malveillantes de la RPDC, les États-Unis s'associent régulièrement avec les pays du monde entier pour sensibiliser aux cybermenaces de la RPDC en partageant des renseignements et des preuves par le biais de divers canaux, notamment ceux de la diplomatie, des forces armées et des instances judiciaires, et des réseaux de la défense. Afin d'entraver les efforts de la RPDC visant à subtiliser des fonds par des moyens informatiques et de se défendre contre les cyberactivités malveillantes de celle-ci, les États-Unis invitent instamment les pays à renforcer les défenses de leurs réseaux, à mettre fin aux coentreprises dans des pays tiers et à expulser de manière conforme au droit international applicable les travailleurs des technologies de l'information (TI) nord-coréens se trouvant sur leur territoire. Une résolution du Conseil de sécurité des Nations Unies de 2017 exige de tous les États Membres qu'ils rapatrient les ressortissants de la RPDC qui perçoivent des revenus sur leur territoire, y inclus les travailleurs des TI, au 22 décembre 2019 au plus tard. Les États-Unis s'emploient également à renforcer les capacités des gouvernements étrangers et du secteur privé de repérer les cybermenaces de la RPDC, de s'en défendre, d'enquêter sur elles, d'entamer des poursuites et d'y répondre, et de participer aux efforts internationaux visant à assurer la stabilité du cyberespace.

Conséquences des comportements interdits ou passibles de sanctions

Les particuliers et les entités qui concourent à des activités de la RPDC liées à l'informatique ou qui soutiennent ces activités, y inclus au traitement de transactions financières en rapport avec ces activités, doivent savoir qu'ils s'exposent à des conséquences éventuelles en se livrant à des comportements interdits ou passibles de sanctions.

Le Bureau du contrôle des avoirs étrangers (OFAC) du département du Trésor a le pouvoir d'imposer des sanctions à toute personne dont il est déterminé qu'elle a, entre autres :

- Mené des activités significatives nuisant à la cybersécurité pour le compte du gouvernement de la Corée du Nord ou du Parti des travailleurs de Corée;
- Opéré dans le secteur des technologies de l'information (TI) en Corée du Nord;
- Mené certaines autres cyberactivités malveillantes facilitées par des moyens informatiques; ou
- Pris part à au moins une activité significative d'importation de puis la Corée du Nord et d'exportation en Corée du Nord de tous biens, services ou technologie.

En outre, si le secrétaire au Trésor détermine, en consultation avec le secrétaire d'État, qu'une institution financière étrangère a sciemment mené ou facilité des activités commerciales significatives avec la Corée du Nord, ou a sciemment effectué ou facilité une transaction significative avec une personne désignée en vertu d'un décret exécutif en rapport avec la Corée du Nord, ou en vertu du décret exécutif 13382 (Prolifératrices d'armes de destruction massive et

leurs soutiens) pour une activité en rapport avec la Corée du Nord, cette institution peut, entre autres restrictions potentielles, être privée de l'aptitude à disposer d'un compte correspondant ou d'un compte de passage aux États-Unis.

L'OFAC enquête sur les violations apparentes de ses règlements en matière de sanctions et exerce un pouvoir d'exécution, ainsi qu'il est énoncé dans les Directives sur l'application des sanctions économiques, (appendice A de la partie 501 du titre 31 du Code des règlements fédéraux). Les personnes qui enfreignent les règlements relatifs aux sanctions contre la Corée du Nord (partie 510 du titre 31 du Code des règlements fédéraux) sont passibles d'amendes civiles d'un montant pouvant atteindre la peine maximale prévue par la loi ou le double de la valeur de la transaction effectuée, selon celui de ces montants qui est le plus élevé.

Le Groupe d'experts note dans son rapport de mi-mandat 2019 que l'usage et les tentatives d'usage de moyens cybernétiques faits par la RPDC pour voler des fonds à des banques et à des sites de change de monnaie numérique pourraient constituer des violations de multiples résolutions du Conseil de sécurité des Nations Unies (à savoir les paragraphes 8 d) de la résolution 1718, 8 et 11 de la résolution 2094, et 32 de la résolution 2270). Les résolutions du Conseil de sécurité visant la RPDC prévoient également divers mécanismes pour encourager le respect des sanctions imposées par les Nations Unies à la RPDC. C'est ainsi, par exemple, que le Comité des sanctions établi en vertu de la résolution 1718 peut imposer des sanctions ciblées (à savoir des gels d'avoirs et, pour les particuliers, des interdictions de voyager) à toute personne physique ou morale qui a des relations d'affaires avec des entités désignées par les Nations Unies ou qui tourne les sanctions de l'Organisation.

Le département de la Justice entame des poursuites pénales en cas de violation délibérée des lois applicables relatives aux sanctions, telles que la Loi relative aux pouvoirs économiques en situation d'urgence international (paragraphes 1701 et suivants du titre 50 du Code des États-Unis). Quiconque enfreint sciemment ces dispositions est passible de peines pouvant aller jusqu'à 20 ans de prison, d'amendes pouvant aller jusqu'à un million de dollars ou au double du produit brut, selon celui de ces deux montants qui est le plus élevé, et à la saisie de tous les fonds objets de telles transactions. Le département de la Justice entame également des poursuites pénales en cas de violations délibérées de la Loi sur le secret bancaire (BSA) (paragraphes 5318 et 5322 du titre 31 du Code des États-Unis), qui exige notamment que les institutions financières appliquent des programmes efficaces de lutte contre le blanchiment de capitaux et remettent certaines déclarations au Réseau pour la répression des délits financiers (FinCEN). Quiconque enfreint la BSA est passible de peines pour aller jusqu'à 5 ans de prison, une amende pouvant aller jusqu'à 250 000 dollars et la saisie éventuelle des biens en rapport avec les violations. S'il y a lieu, le département de la Justice entame des poursuites pénales contre les sociétés et autres entités qui enfreignent ces dispositions. Il œuvre également avec des partenaires étrangers pour partager les éléments de preuve à l'appui de leurs enquêtes et poursuites pénales mutuelles.

En vertu de l'alinéa k du paragraphe 5318 du titre 31 du Code des États-Unis, le secrétaire au Trésor ou le Procureur général peuvent assigner une institution financière étrangère ayant un compte bancaire correspondant aux États-Unis à produire des dossiers archivés à l'étranger. Lorsque le secrétaire au Trésor ou le procureur général notifient par écrit une institution financière américaine du non-respect d'une telle assignation de la part d'institutions financières

étrangères, l'institution financière américaine est tenue de mettre fin à cette relation de banque correspondante dans les dix jours ouvrables. Faute de ce faire, l'institution financière américaine est passible de sanctions civiles journalières.

Programme de récompenses pour la justice

Si vous disposez de renseignements sur les activités illicites de la RPDC dans le cyberspace et sur ses opérations tant passées qu'en cours, la communication de ces renseignements dans le cadre du Programme de récompenses pour la justice du département d'État pourrait vous donner droit à une récompense de jusqu'à 5 millions de dollars. Pour de plus amples informations, veuillez consulter le site www.rewardsforjustice.net.

ANNEXE I : Information du public et ressources du gouvernement des États-Unis pour contrer les cybermenaces de la RPDC

Évaluations annuelles des menaces mondiales de la communauté du renseignement des États-Unis, du Bureau du directeur du renseignement national. En 2019, la communauté du renseignement des États-Unis a déterminé que d'après ses évaluations, la RPDC fait peser une cybermenace significative sur les institutions financières, constitue toujours une cybermenace significative en matière d'espionnage et reste capable de mener des cyber-attaques perturbatrices. La RPDC continue de faire usage de cybercapacités pour voler des fonds à des institutions financières afin de se procurer des recettes. Au nombre des cyberactivités criminelles de Pyongyang figurent des tentatives de vol, dont le montant dépasse 1,1 milliard de dollars, à des institutions financières du monde entier, avec notamment une cyber-attaque contre la Banque du Bangladesh dont le butin a été estimé à 81 millions de dollars. Le rapport établi sur la question est disponible à l'adresse suivante : https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Rapports techniques de l'Agence de la cybersécurité et de la sécurité de l'infrastructure (Cybersecurity and Infrastructure Security Agency = CISA). Le gouvernement des États-Unis a dénommé « HIDDEN COBRA » (COBRA CACHÉ) les cyberactivités malveillantes de la RPDC. Les rapports sur HIDDEN COBRA fournissent des détails techniques sur les outils et l'infrastructure utilisés par les cyber-acteurs de la RPDC. Ils permettent aux défenseurs de réseau de repérer et de réduire l'exposition aux cyberactivités malveillantes de la RPDC. Le site web de la CISA contient les mises à jour les plus récentes sur ces menaces persistantes : https://www.us-cert.gov/northkorea.

Par ailleurs, la CISA fournit de vastes connaissances et de nombreuses pratiques sur la cybersécurité et la sécurité de l'infrastructure à ses parties prenantes, partage ces connaissances de manière à améliorer la gestion des risques et les met en pratique pour protéger les fonctions essentielles de la nation. On trouvera ci-dessous des hyperliens vers les ressources de la CISA :

- Protection de l'infrastructure essentielle : https://www.cisa.gov/protecting-critical-infrastructure
- Cybersécurité : https://www.cisa.gov/cyber-safety
- Détection et prévention : https://www.cisa.gov/detection-and-prevention
- Partage de l'information : https://www.cisa.gov/information-sharing-and-awareness
- Observations de la CISA : https://www.cisa.gov/insights
- Lutte contre la cybercriminalité : https://www.cisa.gov/combating-cyber-crime
- Essentiel de la cybersécurité : https://www.cisa.gov/cyber-essentials
- Renseignements utiles : https://www.us-cert.gov/ncas/tips
- Système national de sensibilisation à la cybersécurité : https://www.us-cert.gov/ncas
- Avis relatifs aux systèmes de contrôle industriels : https://www.us-cert.gov/ics
- Déclaration des incidents, de l'hameçonnage, des maliciels et des vulnérabilités : https://www.us-cert.gov/report

Rapports PIN et FLASH du FBI. Les Notifications du FBI à l'industrie privée (PIN) contiennent des informations actuelles qui accroissent la sensibilisation du secteur privé aux

cybermenaces potentielles. Les rapports du Système d'alertes de liaison (FLASH) du FBI contiennent des informations essentielles compilées par le FBI et destinées à être utilisées par des partenaires spécifiques du secteur privé. Ils ont pour objet de communiquer des renseignements exploitables qui aident les professionnels de la cybersécurité et les administrateurs de système à se prémunir des actions malveillantes persistantes des cybercriminels. Si vous repérez une activité suspecte au sein de votre entreprise ou si vous détenez des renseignements relatifs à de telles activités, veuillez prendre contact immédiatement avec FBI CYWATCH. Pour les rapports PIN et FLASH ayant trait aux cybermenaces liées à la RPDC, prière de prendre contact avec le FBI à l'adresse suivante : cywatch@fbi.gov.

- Division des cyberactivités du FBI : https://www.fbi.gov/investigate/cyber
- Programme de l'attaché juridique du FBI : La mission fondamentale de l'attaché juridique du FBI est d'établir et de maintenir la liaison avec les principaux services des forces de l'ordre et de sécurité de certains pays choisis hors des États-Unis. https://www.fbi.gov/contact-us/legal-attache-offices

Communiqués du Cyber-commandement des États-Unis relatifs aux maliciels. Les cyber-forces du département de la Défense surveillent les cyberactivités malveillantes de la RPDC, notamment le déploiement de maliciels qui exploitent les institutions financières, mènent des activités d'espionnage et permettent de mener des cyberactivités malveillantes contre les États-Unis et leurs partenaires. Le Cyber-commandement des États-Unis diffuse périodiquement des informations sur les maliciels, qui signalent les vulnérabilités pour que les entités commerciales, industrielles et gouvernementales défendent leur infrastructure et leurs réseaux contre les activités illicites de la RPDC. Les renseignements sur les maliciels visant à renforcer la cyber-sécurité sont disponibles via les comptes Twitter suivants : @US_CYBERCOM et @CNMF_VirusAlert.

Renseignements sur les sanctions et avis relatifs aux activités financières illicites fournis par le département du Trésor des États-Unis.
Le Centre de ressources en ligne du Bureau du contrôle des avoirs étrangers (Office of Foreign Assets Control - OFAC) du département du Trésor fournit une somme considérable de renseignements sur les sanctions contre la RPDC ainsi que sur les sanctions visant les cyberactivités malveillantes ; on y trouve notamment des avis sur les sanctions, les textes de lois, décrets exécutifs, règles et règlements relatifs à la RPDC et aux sanctions relatives au cyberactivités. L'OFAC a également publié plusieurs listes de questions fréquemment posées (FAQ) concernant les sanctions contre la RPDC, les sanctions relatives aux cyberactivités et la monnaie numérique. Pour toute question sur les règlements et exigences de l'OFAC concernant les sanctions, prière de se mettre en rapport avec l'OFAC via la ligne directe de conformité au 1-800-540-6322 ou par courriel adressé à OFAC_Feedback@treasury.gov.

- Sanctions contre la RPDC
  - https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx
  - FAQ - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#nk
- Sanctions contre les cyberactivités malveillantes
  - https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx

- FAQ - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#cyber
- FAQ sur la monnaie virtuelle - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs

Le Réseau pour la répression des délits financiers (FinCEN) a émis un avis sur l'emploi du système financier international fait par la Corée du Nord (https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a008). Le FinCEN a également émis des avis spécifiques à l'intention des institutions financières tenues de fournir des déclarations sur les activités suspectes, qui donnent des orientations sur les circonstances dans lesquelles les actes de cybercriminalité et/ou les activités criminelles liées à la monnaie numérique doivent faire l'objet de déclarations et sur la façon de les signaler :

- Cybercriminalité
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005
- Activités illicites liées à la monnaie numérique
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a003
- Compromission des courriels d'entreprises
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a005
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003

Le Conseil fédéral d'examen des institutions financières (Federal Financial Institutions Examination Council - FFIEC) a élaboré un Outil d'évaluation de la cybersécurité pour aider les institutions financières à identifier leurs risques et à déterminer leur état de préparation en matière de cybersécurité. Cet outil d'évaluation est disponible à l'adresse suivante : https://www.ffiec.gov/cyberassessmenttool.htm.

ANNEXE II : Rapports du Groupe d'experts des Nations Unies sur les cybermenaces présentées par la RPDC

Rapports du Groupe d'experts du Comité des sanctions 1718 des Nations Unies sur la RPDC. Le Comité des sanctions 1718 du Conseil de sécurité des Nations Unies sur la RPDC est épaulé par un Groupe d'experts qui « réunit, examine et analyse toutes informations » provenant des États Membres, d'organismes compétents des Nations Unies et d'autres parties intéressées sur l'application des mesures énoncées dans les résolutions du Conseil de sécurité des Nations Unies relatives à la Corée du Nord. Le Groupe d'experts émet également des recommandations quant à la façon d'améliorer l'application des sanctions en fournissant au Comité 1718 un rapport de mi-mandat et un rapport final, lesquels rapports sont consultables à l'adresse suivante : https://www.un.org/securitycouncil/fr/sanctions/1718/panel_experts/reports.