مذكرة إرشادية بشأن التهديد السيبراني من قِبل جمهورية كوريا الشعبية الديمقراطية

صدرت بتاريخ: **15 أبريل/ نيسان، 2020**

العنوان: **إرشادات بشأن التهديد السيبراني من قِبل كوريا الشمالية**

تقوم وزارة الخارجية الأمريكية، ووزارة الخزانة، ووزارة الأمن الوطني، ومكتب التحقيقات الفيدرالي بإصدار هذه المذكرة الإرشادية كمصدر شامل حول التهديد السيبراني الذي تشكله كوريا الشمالية بالنسبة للمجتمع الدولي والمدافعين عن الشبكات والجمهور. تسلط هذه المذكرة الإرشادية الضوء على التهديد السيبراني الذي تشكله كوريا الشمالية - المعروفة رسمياً باسم جمهورية كوريا الشعبية الديمقراطية - ويقدم خطوات يتم التوصية بها للتخفيف من التهديد. وعلى وجه الخصوص، يقدم الملحق 1 قائمة بموارد للحكومة الأمريكية متعلقة بالتهديدات السيبرانية لكوريا الشمالية، ويتضمن الملحق 2 رابطاً لتقارير فريق الخبراء التابع للجنة العقوبات المفروضة على كوريا الشمالية المنشأة بموجب قرار الأمم المتحدة رقم 1718.

تهدد الأنشطة السيبرانية الخبيثة التي تشنها كوريا الشمالية الولايات المتحدة والمجتمع الدولي الأوسع نطاقا، وتشكل، على وجه الخصوص، تهديدا كبيراً لسلامة واستقرار النظام المالي الدولي. لقد اعتمدت كوريا الشمالية، تحت ضغط العقوبات الصارمة التي تفرضها الولايات المتحدة والأمم المتحدة، بشكل متزايد على الأنشطة غير المشروعة - بما في ذلك الجرائم السيبرانية – لتوليد إيرادات لأسلحة الدمار الشامل وبرامج الصواريخ الباليستية الخاصة بها. إن الولايات المتحدة تشعر على وجه الخصوص بقلق عميق حيال الأنشطة السيبرانية الخبيثة لكوريا الشمالية، والتي تشير إليها حكومة الولايات المتحـــدة باسم **الكـوبرا الخفيـــة** "HIDDE COBRA ". إن كوريا الشمالية تمتلك القدرة على القيام بأنشطة سيبرانية تخريبية أو مدمرة تؤثر على البنية التحتية الحيوية للولايات المتحدة. وتستخدم كوريا الشمالية أيضاً القدرات السيبرانية للسرقة من المؤسسات المالية، وقد أظهرت نمطاً من النشاط السيبراني المدمر والضار لا يتوافق نهائياً مع الإجماع الدولي المتزايد بشأن ما يشكل سلوكاً مسؤولاً للدولة في الفضاء السيبراني.

تعمل الولايات المتحدة عن كثب مع الدول ذات التفكير المماثل لتركيز الانتباه على سلوك كوريا الشمالية المخرّب أو المدمر أو المزعزع للاستقرار في الفضاء السيبراني وإدانته. على سبيل المثال، عزت أستراليا وكندا ونيوزيلندا والولايات المتحدة والمملكة المتحدة علناً في ديسمبر/ كانون الأول 2017 هجوم الفدية "وانا

كراي 2.0 - WannaCry 2.0" إلى كوريا الشمالية وشجبت النشاط السيبراني الضار وغير المسؤول لكوريا الشمالية. وأصدرت الدنمارك واليابان بيانات داعمة للإدانة المشتركة لهجوم الفدية "وانا كراي" المدمر، والذي أثر على مئات الآلاف من أجهزة الكمبيوتر حول العالم في مايو/ أيار 2017.

من الضروري أن يبقى المجتمع الدولي والمدافعون عن الشبكات والجمهور يقظين وأن يعملوا معاً للتخفيف من التهديد السيبراني الذي تشكله كوريا الشمالية.

الأنشطة السيبرانية الخبيثة لجمهورية كوريا الشعبية الديمقراطية التي تستهدف القطاع المالي

تخضع العديد من الجهات الفاعلة السيبرانية التابعة لكوريا الشمالية لكيانات مدرجة من قِبل الأمم المتحدة والولايات المتحدة، مثل مكتب الاستطلاع العام. وتتكون الجهات الفاعلة السيبرانية التي ترعاها كوريا الشمالية بالأساس من المتسللين وخبراء التشفير ومطوري البرمجيات الذين يقومون بالتجسس والسرقة المُمكَّنة سيبرانياً التي تستهدف المؤسسات المالية وتبادل العملات الرقمية والعمليات ذات الدوافع السياسية ضد شركات الإعلام الأجنبية. إنهم يطورون وينشرون مجموعة واسعة من أدوات البرمجيات الخبيثة حول العالم لتمكين هذه الأنشطة ولقد تطورت هذه الأدوات بشكل كبير. وتشمل الأساليب الشائعة لزيادة الإيرادات بشكل غير مشروع من قِبل الجهات الفاعلة السيبرانية التي ترعاها كوريا الشمالية، ما يلي على سبيل المثال لا الحصر:

العمليات المُمكَّنة سيبرانياً للسرقة المالية وغسيل الأموال. يشير تقرير منتصف المدة لعام 2019 الصادر عن فريق الخبراء التابع للجنة المنشأة بموجب قرار مجلس الأمن رقم 1718 (تقرير منتصف المدة لفريق الخبراء لعام 2019) إلى أن كوريا الشمالية قادرة بشكل متزايد على توليد الإيرادات على الرغم من عقوبات مجلس الأمن الدولي وذلك باستخدام الأنشطة السيبرانية الخبيثة لسرقة المؤسسات المالية من خلال الأدوات والتكتيكات التي تطورت بشكل كبير. ويشير تقرير منتصف المدة لفريق الخبراء لعام 2019 إلى أنه في بعض الحالات امتدت هذه الأنشطة السيبرانية الخبيثة أيضاً إلى غسيل الأموال عبر ولايات قضائية متعددة. ويشير تقرير منتصف المدة لفريق الخبراء لعام 2019 إلى أن الفريق كان يحقق في العشرات من عمليات السرقة المُمكَّنة سيبرانياً المشتبه في قيام كوريا الشمالية بها، وأنه حتى أواخر عام 2019، حاولت كوريا الشمالية سرقة ما يصل إلى 2 مليار دولار من خلال هذه الأنشطة السيبرانية غير المشروعة. وتتوافق الادعاءات في شكوى المصادرة لوزارة العدل في مارس/ آذار 2020 مع أجزاء من النتائج التي توصل إليها فريق الخبراء. على وجه التحديد، زعمت شكوى المصادرة كيف استخدمت الجهات الفاعلة السيبرانية التابعة لكوريا الشمالية البنية التحتية لكوريا الشمالية لتعزيز مؤامرتها لاختراق تبادل العملات الرقمية وسرقة مئات الملايين من الدولارات بالعملة الرقمية وغسيل الأموال.

حملات الابتزاز. كما قامت الجهات الفاعلة السيبرانية التابعة لكوريا الشمالية بحملات ابتزاز ضد كيانات في دول أخرى من خلال اختراق شبكة الكيان والتهديد بإغلاقها ما لم يدفع الكيان فدية. وفي بعض الحالات، طالبت الجهات الفاعلة السيبرانية التابعة لكوريا الشمالية بقيام الضحايا بدفع مبالغ مالية تحت ستار ترتيبات استشارية مدفوعة الأجر وطويلة الآجل من أجل ضمان عدم حدوث مثل هذا النشاط السيبراني الخبيث في المستقبل. كما تم دفع أموال للجهات الفاعلة السيبرانية التابعة لكوريا الشمالية لاختراق المواقع الالكترونية وابتزاز اهداف لصالح عملاء من دول أخرى.

اختراق التشفير "كريبتو جاكينج" - Cryptojacking". يشير تقرير منتصف المدة لفريق الخبراء لعام 2019 أن فريق الخبراء يحقق أيضاً في استخدام كوريا الشمالية لبرمجية "اختراق التشفير- كريبتو جاكينج"، واختراق التشفير هو مخطط لاختراق جهاز الضحية وسرقة موارد الحوسبة الخاصة به لسرقة العملة الرقمية. ولقد حدد فريق الخبراء العديد من الحوادث التي أرسلت فيها أجهزة الكمبيوتر المصابة ببرمجيات خبيثة لاختراق التشفير الأصول الملغومة - معظمها عملات رقمية معززة لعدم الكشف عن الهوية (يشار إليها أحياناً باسم "عملات الخصوصية") - إلى الخوادم الموجودة في كوريا الشمالية، بما في ذلك في جامعة كيم إيل سونغ في بيونغ يانغ.

تسلط هذه الأنشطة الضوء على استخدام كوريا الشمالية لوسائل مُمكَّنة سيبرانياً لتوليد الإيرادات مع التخفيف من تأثير العقوبات وإظهار أن كوريا الشمالية تستطيع اختراق أي دولة واستغلالها. ووفقاً لتقرير منتصف المدة لفريق الخبراء لعام 2019، فإن فريق الخبراء يحقق أيضاً في أنشطة مثل محاولات مخالفة عقوبات مجلس الأمن الدولي على كوريا الشمالية.

العمليات السيبرانية المنسوبة علناً إلى جمهورية كوريا الشعبية الديمقراطية من قِبل حكومة الولايات المتحدة

استهدفت كوريا الشمالية بشكل متكرر شبكات الولايات المتحدة والشبكات الحكومية والعسكرية الأخرى، بالإضافة إلى الشبكات ذات الصلة بالكيانات الخاصة والبنية التحتية الحيوية، وذلك لسرقة البيانات والقيام بأنشطة سيبرانية تخريبية ومدمرة. وقد نسبت حكومة الولايات المتحدة علناً حتى الآن الحوادث السيبرانية التالية إلى الجهات الفاعلة السيبرانية والمتآمرين معها الذين ترعاهم كوريا الشمالية:

- ***شركة سوني بيكتشرز "Sony Pictures"***. في نوفمبر/ تشرين الثاني 2014، زُعم أن الجهات الفاعلة السيبرانية التي ترعاها كوريا الشمالية قد شنت هجوماً سيبرانياً على شركة "سوني بيكتشرز انترتنمينت" ردًا على فيلم "المقابلة" لعام 2014. إذ اخترقت الجهات الفاعلة السيبرانية التابعة لكوريا الشمالية شبكة الشركة لسرقة بيانات سرية، وهددوا المسؤولين التنفيذيين والموظفين في الشركة وألحقوا الضرر بالآلاف من أجهزة الكمبيوتر.
    - تحديث مكتب التحقيقات الفيدرالي حول تحقيقات شركة سوني (19 ديسمبر/ كانون الأول، 2014)
      https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation
    - الشكوى الجنائية لوزارة العدل بخصوص المبرمج المدعوم من نظام كوريا الشمالية (6 سبتمبر/ أيلول، 2018)
      https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***سرقة بنك بنغلاديش***. يُزعم أن الجهات الفاعلة السيبرانية التي ترعاها كوريا الشمالية حاولت في فبراير/ شباط 2016 سرقة مليار دولار على الأقل من المؤسسات المالية في جميع أنحاء العالم ويُزعم أنها سرقت 81 مليون دولار من بنك بنغلاديش من خلال معاملات غير مصرح بها على

شبكة جمعية الاتصالات المالية العالمية بين البنوك (سويفت). ووفقًا للشكوى، وصلت الجهات الفاعلة السيبرانية التابعة لكوريا الشمالية إلى محطات الكمبيوتر الخاصة ببنك بنغلاديش التي كانت تتعامل مع شبكة سويفت، وذلك بعد اختراق شبكة الكمبيوتر الخاصة بالبنك عبر رسائل البريد الإلكتروني التصيدية التي استهدفت موظفي البنك. ثم قامت الجهات الفاعلة السيبرانية التابعة لكوريا الشمالية بإرسال رسائل مصداقية احتيالية من سويفت توجه بنك الاحتياطي الفيدرالي في نيويورك لتحويل الأموال من حساب الاحتياطي الفيدرالي لبنك بنغلاديش إلى الحسابات التي يسيطر عليها المتآمرون.

- الشكوى الجنائية لوزارة العدل بخصوص المبرمج المدعوم من نظام كوريا الشمالية (6 سبتمبر/ أيلول، 2018)
https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***برنامج وانا كراي 2.0*** "***WannaCry 2.0***". قامت الجهات الفاعلة السيبرانية التي ترعاها كوريا الشمالية بتطوير برنامج الفدية المعروف باسم "وانا كراي 2.0"، بالإضافة إلى نسختين سابقتين من البرنامج. في مايو/ أيار 2017، أصاب برنامج الفدية "وانا كراي 2.0" مئات الآلاف من أجهزة الكمبيوتر في المستشفيات والمدارس والشركات والمنازل في أكثر من 150 دولة. يقوم برنامج الفدية "وانا كراي 2.0" بتشفير بيانات جهاز الكمبيوتر المصاب ويسمح للجهات الفاعلة السيبرانية بالمطالبة بدفع فدية بالعملة الرقمية "بيتكوين – Bitcoin". ولقد قامت وزارة الخزانة الأمريكية بإدراج مبرمج كمبيوتر كوري شمالي واحد لدوره في مؤامرة "وانا كراي 2.0"، بالإضافة إلى دوره في الهجوم السيبراني على شركة "سوني بكتشرز" وسرقة بنك بنغلاديش، كما قامت بإدراج المنظمة التي عمل بها.

- التحذير الفني لوكالة الأمن السيبراني وأمن البنية التحتية: المؤشرات المرتبطة ببرنامج الفدية "وانا كراي" (12 مايو/ أيار، 2017)
https://www.us-cert.gov/ncas/alerts/TA17-132A
- الموجز الصحفي للبيت الأبيض حول إسناد برنامج الفدية "وانا كراي" (19 ديسمبر/ كانون الأول، 2017)
https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/
- الشكوى الجنائية لوزارة العدل بخصوص المبرمج المدعوم من نظام كوريا الشمالية (6 سبتمبر/ أيلول، 2018)
https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and
- وزارة الخزانة الأمريكية تستهدف كوريا الشمالية بسبب هجمات سيبرانية متعددة (6 سبتمبر/ ايلول، 2018)
https://home.treasury.gov/news/press-releases/sm473

- ***حملة الكاش السريع "FASTCash".*** منذ أواخر عام 2016، استخدمت الجهات الفاعلة السيبرانية التي ترعاها كوريا الشمالية مخطط للسحب النقدي من أجهزة الصراف الآلي يُعرف باسم "الكاش السريع" لسرقة عشرات الملايين من الدولارات من أجهزة الصراف الآلي في آسيا وأفريقيا. يخترق مخطط "الكاش السريع" عن بُعد خوادم تطبيقات مفتاح الدفع داخل البنوك من أجل تسهيل المعاملات الاحتيالية. لقد مكّنت الجهات الفاعلة السيبرانية التابعة لكوريا الشمالية في حادثة واحدة عام 2017 عمليات سحب نقدي من أجهزة الصراف الآلي الموجودة في أكثر من 30 دولة مختلفة في وقت واحد. وفي حادثة أخرى في عام 2018، مكّنت الجهات الفاعلة السيبرانية التابعة لكوريا الشمالية عمليات سحب نقدي من أجهزة الصراف الآلي في 23 دولة مختلفة في وقت واحد.

  - التحذير الفني لوكالة الأمن السيبراني وأمن البنية التحتية بشأن حملة الكاش السريع (2 أكتوبر/ تشرين الأول، 2018) https://www.us-cert.gov/ncas/alerts/TA18-275A
  - تقرير تحليل البرامج الضارة لوكالة الأمن السيبراني وأمن البنية التحتية: الكاش السريع – البرامج الضارة ذات الصلة (2 أكتوبر/ تشرين الأول، 2018) https://www.us-cert.gov/ncas/analysis-reports/AR18-275A

- ***اختراق تبادل العملات الرقمية***: كما هو مفصل في الادعاءات المنصوص عليها في شكوى وزارة العدل بشأن المصادرة العينية، اخترقت الجهات الفاعلة السيبرانية التي ترعاها كوريا الشمالية في أبريل/ نيسان 2018 تبادل للعملات الرقمية وسرقوا ما يقرب من 250 مليون دولار من العملة الرقمية. ووصفت الشكوى كذلك كيف تم غسيل الأصول المسروقة من خلال مئات المعاملات الرقمية الآلية، لإخفاء أصول الأموال، في محاولة لمنع سلطات إنفاذ القانون من تتبع الأصول. ويُزعم في الشكوى أن أثنين من المواطنين الصينيين قاموا فيما بعد بغسيل الأصول نيابة عن مجموعة كوريا الشمالية وحصلوا على حوالي 91 مليون دولار من الحسابات التي تسيطر عليها كوريا الشمالية، بالإضافة إلى 9.5 مليون دولار إضافية من اختراق تبادل آخر. ولقد قامت وزارة الخزانة الأمريكية في مارس/ آذار 2020 بإدراج الشخصين تحت سلطات العقوبات السيبرانية والعقوبات على كوريا الشمالية، وذلك بالتزامن مع إعلان وزارة العدل أن الشخصين قد تم اتهامهما سابقاً بتهمة غسيل الأموال وتحويل الأموال غير المرخص به، وأن 113 من حسابات العملات الرقمية قد خضعت للمصادرة.

  - عقوبات وزارة الخزانة الأمريكية ضد الأفراد الذين يقومون بغسيل العملة المشفرة لمجموعة لازاروس (2 مارس/ أذار، 2020) https://home.treasury.gov/news/press-releases/sm924
  - لائحة اتهام وزارة العدل الأمريكية لاثنين من المواطنين الصينيين المتهمان بغسيل العملة الرقمية من شكوى اختراق التبادل والمصادرة المدنية (2مارس/ آذار، 2020) https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack

تدابير لمكافحة التهديد السيبراني من قِبل جمهورية كوريا الشعبية الديمقراطية

تستهدف كوريا الشمالية البنية التحتية السيبرانية على مستوى العالم لتوليد الإيرادات لأولويات نظامها، بما في ذلك برامج أسلحة الدمار الشامل. نحن نحث بشدة الحكومات والصناعة والمجتمع المدني والأفراد على اتخاذ جميع الإجراءات ذات الصلة أدناه لحماية أنفسهم من التهديد السيبراني لكوريا الشمالية والتصدي له:

- **رفع الوعي بالتهديد السيبراني من قِبل جمهورية كوريا الشعبية الديمقراطية.** يؤدي تسليط الضوء على خطورة ونطاق وتنوع الأنشطة السيبرانية الخبيثة التي تقوم بها كوريا الشمالية إلى زيادة الوعي العام بالتهديد عبر القطاعين العام والخاص وتعزيز اعتماد وتنفيذ تدابير مناسبة للوقاية وتخفيف المخاطر.

- **تقاسم المعلومات التقنية حول التهديد السيبراني من قِبل جمهورية كوريا الشعبية الديمقراطية.** إن تبادل المعلومات على المستويين الوطني والدولي للكشف عن التهديد السيبراني لكوريا الشمالية واتخاذ الإجراءات الدفاعية ضده سيمكن من تعزيز الأمن السيبراني للشبكات والأنظمة. ينبغي تقاسم أفضل الممارسات مع الحكومات والقطاع الخاص. يجوز وفقاً لأحكام قانون تقاسم معلومات الأمن السيبراني لعام 2015 (القانون الأمريكي رقم 6 الأقسام 1501-1510 - 6 U.S.C. §§ 1501–1510) للكيانات غير الفيدرالية تقاسم مؤشرات التهديدات السيبرانية والتدابير الدفاعية المتعلقة ببرنامج **الكوبرا الخفية** مع الكيانات الفيدرالية وغير الفيدرالية.

- **تنفيذ وتعزيز أفضل ممارسات الأمن السيبراني.** سيؤدي اتخاذ تدابير - فنية وسلوكية - لتعزيز الأمن السيبراني إلى جعل البنية التحتية السيبرانية الأمريكية والعالمية أكثر أماناً ومرونة. يجب على المؤسسات المالية، بما في ذلك شركات الخدمات المالية، اتخاذ خطوات مستقلة للحماية من الأنشطة السيبرانية لكوريا الشمالية. ويجوز أن تتضمن هذه الخطوات، على سبيل المثال لا الحصر، تبادل معلومات التهديد من خلال القنوات الحكومية و/ أو قنوات الصناعة، وتقسيم الشبكات لتقليل المخاطر، والحفاظ على نسخ احتياطية منتظمة للبيانات، وإجراء تدريبات للتوعية بأساليب الهندسة الاجتماعية الشائعة، وتنفيذ سياسات تحكم تقاسم المعلومات والوصول إلى الشبكات، ووضع خطط للاستجابة للحوادث السيبرانية. ويقدم نموذج نضج قدرات الأمن السيبراني لوزارة الطاقة الأمريكية وإطار الأمن السيبراني للمعهد الوطني للمعايير والتقنية إرشادات حول تطوير وتنفيذ ممارسات قوية للأمن السيبراني. وكما هو موضح في الملحق 1، توفر وكالة الأمن السيبراني وأمن البنية التحتية موارد واسعة، بما في ذلك التنبيهات التقنية وتقارير تحليل البرامج الضارة لتمكين المدافعين عن الشبكات من تحديد وتقليل التعرض للأنشطة السيبرانية الخبيثة.

- **إخطار سلطات إنفاذ القانون.** إذا اشتبهت إحدى المنظمات في أنها كانت ضحية لنشاط سيبراني خبيث، ناشئ من كوريا الشمالية أو غير ذلك، فمن الأهمية بمكان إخطار سلطات إنفاذ القانون في الوقت المناسب. إن هذا لا يمكّن فقط من الإسراع بالتحقيق، ولكنه يمكن أن يؤدي أيضاً في حالة وقوع جريمة مالية إلى زيادة فرص استرداد أي أصول مسروقة.

صادرت سلطات إنفاذ القانون الأمريكية ملايين الدولارات من العملة الرقمية التي سرقتها الجهات الفاعلة السيبرانية التابعة لكوريا الشمالية. يتم تشجيع جميع أنواع المؤسسات المالية، بما

في ذلك شركات الخدمات المالية، على التعاون قبل بدء المعاملات المالية من خلال الامتثال لطلبات سلطات إنفاذ القانون الأمريكية للحصول على معلومات بشأن هذه التهديدات السيبرانية، وبعد انتهاء المعاملات المالية من خلال تحديد الأصول القابلة للمصادرة عند استلام طلب من سلطات إنفاذ القانون الأمريكية أو أوامر من محكمة أمريكية، ومن خلال التعاون مع سلطات إنفاذ القانون الأمريكية لدعم مُصادرة هذه الأصول.

- **تعزيز الامتثال لمكافحة غسيل الأموال/ مكافحة تمويل الإرهاب/ مكافحة تمويل انتشار الاسلحة**. يجب على الدول أن تنفذ بسرعة وفعالية معايير فرقة العمل المعنية بالإجراءات المالية بشأن مكافحة غسيل الأموال ومكافحة تمويل الإرهاب ومكافحة تمويل الانتشار. ويشمل ذلك التأكد من استخدام المؤسسات المالية والكيانات الأخرى المشمولة تدابير تخفيف المخاطر بما يتماشى مع معايير فرقة العمل المعنية بالإجراءات المالية والبيانات والارشادات العامة للفرقة. وعلى وجه التحديد، دعت فرقة العمل المعنية بالإجراءات المالية جميع الدول إلى تطبيق تدابير مضادة لحماية النظام المالي الدولي من المخاطر المستمرة لغسيل الأموال وتمويل الإرهاب وتمويل انتشار الأسلحة الناشئة من كوريا الشمالية[1]. ويشمل ذلك تقديم المشورة لجميع المؤسسات المالية والكيانات الأخرى المشمولة لإيلاء اهتمام خاص للعلاقات والمعاملات التجارية مع كوريا الشمالية، بما في ذلك الشركات والمؤسسات المالية لكوريا الشمالية ومن يعمل نيابة عنها. وتماشيا مع الفقرة (33) من منطوق قرار مجلس الأمن الدولي رقم (2270)، يجب على الدول الأعضاء إغلاق فروع بنوك كوريا الشمالية والشركات التابعة لها والمكاتب التمثيلية الموجودة داخل أراضيها وإنهاء علاقات المراسلة مع بنوك كوريا الشمالية.

بالإضافة إلى ذلك، قامت فرقة العمل المعنية بالإجراءات المالية في شهر يونيو/ حزيران 2019 بتعديل معاييرها لمطالبة جميع البلدان بوضع لوائح تنظيمية لمزودي خدمة الأصول الرقمية والاشراف عليهم، بما في ذلك تبادل العملات الرقمية، والتخفيف من المخاطر عند الانخراط في معاملات العُملات الرقمية. ويجب أن يظل مزودو خدمة الأصول الرقمية متيقظين للتغيرات في أنشطة العملاء، حيث يمكن استخدام أعمالهم التجارية لتسهيل غسيل الأموال وتمويل الإرهاب وتمويل الانتشار . إن الولايات المتحدة قلقة بشكل خاص بشأن المنصات التي توفر أنشطة الدفع وخدمات الحسابات مجهولة الهوية وذلك دون مراقبة المعاملات، والإبلاغ عن الأنشطة المشبوهة، والعناية الواجبة للعملاء، من بين التزامات أخرى.

يجب على المؤسسات المالية الأمريكية، بما في ذلك مزودي خدمة الأصول الرقمية الموجودين في الخارج الذين يقومون بأعمال تجارية كليا أو بشكل جزئي كبير في الولايات المتحدة، والشركات والأشخاص الآخرين المشمولين التأكد من امتثالهم لالتزاماتهم التنظيمية بموجب قانون السرية المصرفية (Bank Secrecy Act) (على النحو الذي يتم تنفيذه من خلال لوائح جهاز مكافحة الجرائم المالية (FinCEN) في وزارة الخزانة الأمريكية، العنوان رقم (31) من الفصل العاشر من قانون اللوائح الفيدرالية) . وتشمل هذه الالتزامات بالنسبة للمؤسسات المالية وضع والحفاظ على برامج فعالة لمكافحة غسيل الأموال يتم تصميمها بشكل معقول لمنع استخدام شركات الخدمات المالية لتسهيل غسيل الأموال وتمويل الأنشطة الإرهابية، بالإضافة إلى تحديد المعاملات المشبوهة

[1] *يمكن الاطلاع على الدعوة الكاملة لفرقة العمل المعنية بالإجراءات المالية حول كوريا الشمالية هنا:* https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html.

والإبلاغ عنها، بما في ذلك تلك التي تم القيام بها أو تأثرت أو تم تسهيلها من خلال الأنشطة السيبرانية أو التمويل غير المشروع الذي ينطوي على أصول رقمية، وذلك ضمن الأنشطة المشبوهة التي يتم إبلاغ جهاز مكافحة الجرائم المالية عنها.

التعاون الدولي. لمواجهة الأنشطة السيبرانية الخبيثة لكوريا الشمالية، تشارك الولايات المتحدة بانتظام مع الدول حول العالم لزيادة الوعي بالتهديد السيبراني الذي تشكله كوريا الشمالية من خلال تبادل المعلومات والأدلة عبر القنوات الدبلوماسية والعسكرية وقنوات إنفاذ القانون والقضاء وشبكات الدفاع والقنوات الأخرى. ولإعاقة جهود كوريا الشمالية لسرقة الأموال من خلال الوسائل السيبرانية ولمواجهة الأنشطة السيبرانية الخبيثة لكوريا الشمالية، تحث الولايات المتحدة الدول بقوة على تعزيز شبكات الدفاع، وإغلاق المشاريع المشتركة مع كوريا الشمالية في الدول الاخرى، وطرد موظفي تكنولوجيا المعلومات التابعين لكوريا الشمالية الموجودين في الخارج بطريقة تتوافق مع القانون الدولي المعمول به. لقد طالب قرار لمجلس الأمن الدولي صدر في عام 2017 من جميع الدول الأعضاء إعادة رعايا كوريا الشمالية الذين يكسبون دخلا في الخارج، بما في ذلك موظفي تكنولوجيا المعلومات، بحلول 22 ديسمبر/ كانون الأول 2019. وتسعى الولايات المتحدة أيضا إلى تعزيز قدرة الحكومات الأجنبية والقطاع الخاص على فهم التهديدات السيبرانية لكوريا الشمالية والتعرف عليها والدفاع ضدها والتحقيق فيها وملاحقتها والرد عليها، والمشاركة في الجهود الدولية للمساعدة في ضمان استقرار الفضاء السيبراني.

عواقب الانخراط في سلوك محظور أو خاضع للعقوبات

يجب على الأفراد والكيانات الذين يشاركون في أنشطة سيبرانية تابعة لكوريا الشمالية أو يقومون بدعم تلك الأنشطة، بما في ذلك معالجة المعاملات المالية ذات الصلة، أن يكونوا على دراية بالعواقب المحتملة للمشاركة في سلوك محظور أو خاضع للعقوبات.

يمتلك مكتب مراقبة الأصول الأجنبية التابع لوزارة الخزانة الأمريكية سلطة فرض عقوبات على أي شخص يثبت، من بين أمور أخرى، انه قام بالآتي:

- شارك في أنشطة هامة تقوض الأمن السيبراني نيابة عن حكومة كوريا الشمالية أو حزب العمال الكوري؛
- عمِلَ في صناعة تكنولوجيا المعلومات في كوريا الشمالية؛
- شارك في أنشطة خبيثة معينة أخرى مُمكّنة سيبرانياً؛ أو
- شارك في عملية استيراد أو تصدير واحدة هامة على الأقل لأي سلع أو خدمات أو تكنولوجيا من أو إلى كوريا الشمالية.

بالإضافة إلى ذلك، إذا قرر وزير الخزانة الأمريكي، بالتشاور مع وزير الخارجية، أن مؤسسة مالية أجنبية قامت أو سهلت عن علم تجارة هامة مع كوريا الشمالية، أو قامت أو سهلت عن علم مُعاملة تجارية هامة نيابة عن شخص تم إدراجه بموجب أمر تنفيذي مرتبط بكوريا الشمالية، أو بموجب الأمر التنفيذي رقم 13382 (ناشرو أسلحة الدمار الشامل ومن يدعمهم) لأنشطة تتعلق بكوريا الشمالية، قد تفقد هذه المؤسسة، من بين قيود أخرى محتملة، القدرة على الاحتفاظ بحسابات مراسلة أو حسابات دفع مراسلة في الولايات المتحدة الأمريكية.

يحقق مكتب مراقبة الأصول الأجنبية في الانتهاكات الواضحة للوائح العقوبات الخاصة به ويمارس سلطة الإنفاذ على النحو المبين في المبادئ التوجيهية لإنفاذ العقوبات الاقتصادية، العنوان رقم 31 من قانون اللوائح الفيدرالية، القسم 501، الملحق أ. قد يواجه الأشخاص الذين ينتهكون لوائح العقوبات المفروضة على كوريا الشمالية، العنوان رقم 31 من قانون اللوائح الفيدرالية، القسم 501، عقوبات مالية مدنية تصل إلى الحد الأقصى للعقوبة القانونية المطبقة أو ضعف قيمة المعاملة الأساسية.

يشير تقرير منتصف المدة لفريق الخبراء لعام 2019 إلى أن استخدام كوريا الشمالية، ومحاولتها استخدام، الوسائل الممكّنة سيبرانيا لسرقة الأموال من البنوك وتبادل العملات الرقمية قد ينتهك العديد من قرارات مجلس الدولي (*بمعنى*، الفقرة (d 8) من منطوق قرار مجلس الأمن رقم (1718)، والفقرتان (8) و (11) من منطوق قرار مجلس الأمن رقم (2094)، والفقرة (32) من منطوق قرار مجلس الأمن رقم (2270)). كما توفر قرارات مجلس الأمن ذات الصلة بكوريا الشمالية آليات مختلفة لتشجيع الامتثال للعقوبات المتعلقة بكوريا الشمالية التي تفرضها الأمم المتحدة. فعلى سبيل المثال، قد تفرض اللجنة المنشأة بموجب قرار مجلس الأمن رقم (1718) عقوبات محددة الهدف (*بمعنى*، تجميد الأصول وحظر السفر بالنسبة للأفراد) على أي فرد أو كيان يشارك في معاملة تجارية مع كيانات مُدرجة من قبل الأمم المتحدة أو في التهرب من العقوبات.

تُلاحق وزارة العدل جنائيا الانتهاكات المتعمدة للقوانين السارية للعقوبات، مثل قانون الطوارئ الاقتصادية الدولية (International Emergency Economic Powers Act)، قانون الولايات المتحدة رقم (50)، القسم (1701) وما يليه. وقد يواجه الأشخاص الذين ينتهكون هذه القوانين عن عمد عقوبة تصل إلى 20 عاما من السجن، وغرامات تصل إلى مليون دولار أو ما يعادل ضعف إجمالي الربح، أيهما أكبر، ومصادرة جميع الأموال المتضمنة في مثل هذه المعاملات. كما تلاحق وزارة العدل جنائيا الانتهاكات المتعمدة لقانون السرية المصرفية، قانون الولايات المتحدة رقم (31)، القسمان (5318) و (5322) الذي يطلب من المؤسسات المالية، من بين أمور أخرى، الحفاظ على برامج فعالة لمكافحة غسيل الأموال وتقديم تقارير معينة إلى جهاز مكافحة الجرائم المالية. قد يواجه الأشخاص الذين ينتهكون قانون السرية المصرفية السجن لمدة تصل إلى 5 سنوات، وغرامة تصل إلى 250,000 دولار، ومصادرة محتملة للممتلكات المتضمنة في الانتهاكات.
وستقوم وزارة العدل، عند الاقتضاء، بالملاحقة الجنائية للشركات والكيانات الأخرى التي تنتهك هذه القوانين. وتعمل وزارة العدل أيضا مع الشركاء الأجانب لتبادل الأدلة لدعم التحقيقات والملاحقات الجنائية لبعضهم البعض.

بموجب قانون الولايات المتحدة رقم (31)، القسم (k)5318، يجوز لوزير الخزانة أو وزير العدل استدعاء مؤسسة مالية أجنبية تحتفظ بحساب بنك مراسل في الولايات المتحدة للحصول على السجلات المخزنة في الخارج. وعندما يقدم وزير الخزانة أو وزير العدل اشعارا كتابيا إلى مؤسسة مالية أمريكية بأن مؤسسة مالية أجنبية قد فشلت في الامتثال لمثل هذا الاستدعاء، يجب على المؤسسة المالية الأمريكية إنهاء العلاقة البنكية المراسلة في غضون عشرة أيام عمل. وقد يؤدي عدم القيام بذلك إلى إخضاع المؤسسات المالية الأمريكية لعقوبات مدنية يومية.

<u>برنامج المكافآت من أجل العدالة الخاص بجمهورية كوريا الشعبية الديمقراطية</u>

إذا كانت لديكم معلومات حول أنشطة كوريا الشمالية غير المشروعة في الفضاء السيبراني، بما في ذلك العمليات السابقة أو الجارية، فإن تقديم مثل هذه المعلومات من خلال برنامج المكافآت من اجل العدالة التابع

لوزارة الخارجية الأمريكية يمكن أن يجعلكم مؤهلين لتلقي مكافأة تصل إلى 5 ملايين دولار. للمزيد من التفاصيل، يرجى زيارة الموقع www.rewardsforjustice.net.

الملحق 1: معلومات وموارد للحكومة الأمريكية متاحة للعامة لمواجهة التهديد السيبراني لجمهورية كورية الشعبية الديمقراطية

التقييم السنوي لخبراء الاستخبارات الأمريكية بشأن التهديدات العالمية الصادر عن مكتب مدير الاستخبارات الوطنية. في عام 2019، قدّرَ خبراء الاستخبارات الامريكية أن كوريا الشمالية تشكل تهديدا سيبرانيا كبيرا للمؤسسات المالية، وأنها لا تزال تشكل تهديدا في مجال التجسس السيبراني، وتحتفظ بالقدرة على شن هجمات سيبرانية تخريبية. وتواصل كوريا الشمالية استخدام القدرات السيبرانية للسرقة من المؤسسات المالية لتوليد الإيرادات. وتشمل عمليات الجرائم السيبرانية لبيونغ يانغ محاولات لسرقة أكثر من 1.1 مليار دولار من المؤسسات المالية في جميع أنحاء العالم - بما في ذلك عملية سرقة سيبرانية ناجحة لمبلغ يُقدّر بـ 81 مليون دولار من بنك في بنغلاديش. يمكن الاطلاع على التقرير على الموقع:
https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

التقارير الفنية لوكالة الأمن السيبراني وأمن البنية التحتية. تشير الحكومة الأمريكية إلى الأنشطة السيبرانية الخبيثة التي تقوم بها كوريا الشمالية باسم **الكوبرا الخفية**. وتوفر تقارير **الكوبرا الخفية** تفاصيل فنية حول الأدوات والبنية التحتية المستخدمة من قِبل الجهات الفاعلة السيبرانية التابعة لكوريا الشمالية. وتُمكِّن هذه التقارير المدافعين عن الشبكات من تحديد وتقليل التعرض للأنشطة السيبرانية الخبيثة لكوريا الشمالية.
ويحتوي موقع وكالة الأمن السيبراني وأمن البنية التحتية على آخر التحديثات حول هذه التهديدات المستمرة:
https://www.us-cert.gov/northkorea

بالإضافة إلى ذلك، توفر وكالة الأمن السيبراني وأمن البنية التحتية معارف وممارسات واسعة النطاق في الأمن السيبراني وأمن البنية التحتية للمهتمين بالأمر فيها، وتتقاسم هذه المعارف للتمكين من إدارة المخاطر بشكل أفضل، ووضع هذه المعارف موضع التنفيذ لحماية الوظائف الحيوية في البلاد. وفيما يلي الروابط الالكترونية لموارد وكالة الأمن السيبراني وأمن البنية التحتية:

- حماية البنية التحتية الحيوية: https://www.cisa.gov/protecting-critical-infrastructure
- السلامة السيبرانية: https://www.cisa.gov/cyber-safety
- الكشف والوقاية: https://www.cisa.gov/detection-and-prevention
- تبادل المعلومات: https://www.cisa.gov/information-sharing-and-awareness
- الرؤى الخاصة بوكالة الأمن السيبراني وأمن البنية التحتية: https://www.cisa.gov/insights
- مكافحة الجريمة السيبرانية: https://www.cisa.gov/combating-cyber-crime
- المبادئ السيبرانية الأساسية: https://www.cisa.gov/cyber-essentials
- نصائح: https://www.us-cert.gov/ncas/tips
- النظام الوطني للتوعية السيبرانية: https://www.us-cert.gov/ncas
- إرشادات نظم الرقابة الصناعية: https://www.us-cert.gov/ics
- الإبلاغ عن الحوادث، وعمليات التصيّد، والبرامج الضارة، ونقاط الضعف: https://www.us-cert.gov/report.

الإشعارات المقدمة للقطاع الخاص الصناعي وتقارير نظام تنبيه مسؤولي الاتصال لمكتب التحقيقات الفيدرالي. توفر الإشعارات التي يقدمها مكتب التحقيقات الفيدرالي إلى القطاع الخاص الصناعي معلومات حديثة من شأنها أن تعزز وعي القطاع الخاص بالتهديد السيبراني المحتمل. وتحتوي تقارير مكتب التحقيقات الفيدرالي الخاصة بنظام تنبيه مسؤولي الاتصال على معلومات هامة يجمعها مكتب التحقيقات الفيدرالي لاستخدامها من قِبل شركاء معينين من القطاع الخاص، وهي تهدف إلى تزويد المستلمين بمعلومات استخبارية عملية تساعد المتخصصين في الأمن السيبراني ومُدراء الأنظمة على توفير الحماية من الأعمال الخبيثة المستمرة لمجرمي الفضاء السيبراني. إذا حددتم أي نشاط مريب داخل مؤسستكم أو كان لديكم معلومات ذات صلة، يرجى فوراً الاتصال بقسم مراقبة الجرائم السيبرانية في مكتب التحقيقات الفيدرالي (FBI CYWATCH). وبالنسبة لإشعارات القطاع الخاص الصناعي أو تقارير نظام تنبيه مسؤولي الاتصال المتعلقة بالتهديد السيبراني لكوريا الشمالية، يُرجى الاتصال بـ cywatch@fbi.gov.

- القسم السيبراني في مكتب التحقيقات الفيدرالي: https://www.fbi.gov/investigate/cyber
- برنامج الملحق القانوني لمكتب التحقيقات الفيدرالي: تتمثل المَهَمة الرئيسية لبرنامج الملحق القانوني لمكتب التحقيقات الفيدرالي في تأسيس والحفاظ على الاتصال مع سلطات إنفاذ القانون والخدمات الأمنية الرئيسية في بلدان أجنبية مُعينة. https://www.fbi.gov/contact-us/legal-attache-offices

نشرات المعلومات المتعلقة بالبرمجيات الضارة التي تُصدرها القيادة السيبرانية للولايات المتحدة. تسعى القوات السيبرانية التابعة لوزارة الدفاع الأمريكية بشكل نشط إلى البحث عن الأنشطة السيبرانية الخبيثة لكوريا الشمالية، بما في ذلك برمجياتها الضارة التي تستغل المؤسسات المالية وتقوم بعمليات التجسس وتمكن الأنشطة السيبرانية الخبيثة ضد الولايات المتحدة وشركائها. وتقوم القيادة السيبرانية للولايات المتحدة بنشر معلومات عن البرمجيات الضارة بشكل دوري لتحديد نقاط الضعف لدي الصناعة والحكومة لتتمكن من الدفاع عن بنيتها التحتية وشبكاتها ضد الأنشطة غير المشروعة لكوريا الشمالية. يمكن الاطلاع على معلومات البرمجيات الضارة من أجل تعزيز الأمن السيبراني على حسابي برنامج تويتر التاليين: @US_CYBERCOM و @CNMF_VirusAlert

المعلومات الخاصة بالعقوبات والارشادات المتعلقة بالتمويل غير المشروع الصادرة عن وزارة الخزانة الأمريكية. يوفر مركز الموارد على شبكة الانترنت التابع ***لمكتب مراقبة الأصول الأجنبية*** كم هائل من المعلومات فيما يتعلق بالعقوبات المفروضة على كوريا الشمالية والعقوبات المتعلقة بالأنشطة الخبيثة المُمكّنة سيبرانياً، بما في ذلك المذكرات الإرشادية الخاصة بالعقوبات، والقوانين ذات الصلة، والأوامر التنفيذية، والقواعد، واللوائح المتصلة بكوريا الشمالية والعقوبات المتعلقة بالمجال السيبراني. كما نشر مكتب مراقبة الأصول الأجنبية العديد من الأسئلة الشائعة التي تتعلق بالعقوبات المفروضة على كوريا الشمالية، والعقوبات المتعلقة بالمجال السيبراني، والعملة الرقمية. للأسئلة أو الاستفسارات المتعلقة بلوائح ومتطلبات العقوبات لمكتب مراقبة الأصول الأجنبية، يرجى الاتصال بالخط الساخن للامتثال التابع للمكتب على الرقم: 1-800-540-6322 أو OFAC_Feedback@treasury.gov.

- العقوبات المفروضة على جمهورية كوريا الشعبية الديمقراطية
  - https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx
  - الأسئلة الشائعة: https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#nk
- العقوبات المفروضة على الأنشطة السيبرانية الخبيثة
  - https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx
  - الأسئلة الشائعة: https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#cyber
  - الأسئلة الشائعة حول العملة الافتراضية: https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs

أصدر ***جهاز مكافحة الجرائم المالية*** (***FinCEN***) مذكرة إرشادية حول استخدام كوريا الشمالية للنظام المالي الدولي (https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a008). كما أصدر الجهاز مذكرات إرشادية محددة للمؤسسات المالية حول الالتزام بالإبلاغ عن الأنشطة المشتبه فيها وتوفر هذه المذكرات الإرشادية توجيهات حول وقت وكيفية الإبلاغ عن الجريمة السيبرانية و/أو النشاط الاجرامي المتعلق بالعملة الرقمية:

- الجرائم السيبرانية
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005
- الأنشطة غير المشروعة المتعلقة بالعملة الرقمية
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a003
- اختراق البريد الالكتروني للشركات التجارية
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a005
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003

طور ***المجلس الفيدرالي لفحص المؤسسات المالية*** (***FFIEC***) أداة لتقييم الأمن السيبراني لمساعدة المؤسسات المالية على تحديد مخاطرها وتحديد مدى استعدادها في مجال الأمن السيبراني. يمكن الاطلاع على أداة التقييم على الموقع: https://www.ffiec.gov/cyberassessmenttool.htm

الملحق 2: تقارير فريق الخبراء التابع للأمم المتحدة حول التهديد السيبراني من قِبل جمهورية كوريا الشعبية الديمقراطية

تقارير فريق الخبراء التابع للجنة العقوبات المفروضة على كوريا الشمالية المنشأة بموجب قرار الأمم المتحدة رقم 1718. يتم دعم لجنة العقوبات المفروضة على كوريا الشمالية المنشأة بموجب قرار مجلس الأمن الدولي رقم 1718 بواسطة فريق من الخبراء، يقوم "بجمع وفحص وتحليل المعلومات" من الدول الأعضاء في الأمم المتحدة، وهيئات الأمم المتحدة ذات الصلة، والأطراف الأخرى بشأن تنفيذ التدابير المحددة في قرارات مجلس الأمن الدولي ضد كوريا الشمالية. ويقدم الفريق أيضا توصيات بشأن كيفية تحسين تنفيذ العقوبات من خلال تقديم تقرير منتصف المدة وتقرير نهائي إلى اللجنة المنشأة بموجب القرار رقم 1718. يمكن الاطلاع على هذه التقارير على الموقع:
https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports