العقوبات المالية المستهدِفة الصادرة عن الأمم المتحدة ضدّ تمويل الإرهاب وانتشار أسلحة الدمار الشامل

ورقة التطبيقات

المحتوى

مقدمة

يفرض مجلس الأمن التابع للأمم المتحدة بموجب الفصل السابع من ميثاق الأمم المتحدة تطبيق 14 نظام عقوبات لغرض حفظ السلام والأمن من خلال قرارات مجلس الأمن ولجان العقوبات. وتركّز هذه الأنظمة على دعم الحل السياسي للنزاعات ومنع انتشار الأسلحة النووية ومكافحة الإرهاب.

يركّز هذا المستند على أنظمة العقوبات التابعة لمجلس الأمن التالية فقط:

- الإرهاب وتمويل الإرهاب في ما يتعلّق بـ:
  - تنظيم الدولة الإسلامية في العراق والشام (داعش) وتنظيم القاعدة وما يرتبط بهما من أفراد وجماعات ومؤسسات وكيانات
  - تنظيم طالبان وما يرتبط به من أفراد وجماعات ومؤسسات وكيانات.
- انتشار أسلحة الدمار الشامل وتمويله في ما يتعلّق بـ:
  - البرامج النووية وتلك المرتبطة بغيرها من أسلحة الدمار الشامل والصواريخ البالستية لجمهورية كوريا الديموقراطية الشعبية
  - البرنامج النووي للجمهورية الإسلامية الإيرانية.

يعرض هذا المستند قضايا وأمثلة تظهر كيف تمّ دعم وتمويل هذه الأنشطة أو الأشخاص أو المجموعات أو الكيانات الخاضعة للعقوبات، ما شكّل مخالفة أو تهرّب من قرارات مجلس الأمن ذات الصلة.

إنّ كافة المعلومات المقدّمة في هذا المستند مأخوذة من المصادر المفتوحة وهي تشمل مجموعة من القضايا والحالات وتهدف إلى إرشاد المؤسسات العامة والخاصة حول التوجّهات والمنهجيات المُستخدمة من قبل الأشخاص أو المجموعات أو الكيانات الخاضعة للعقوبات للالتفاف على قرارات مجلس الأمن. تقع المسؤولية على كلّ مؤسسة بتطبيق التدابير الكافية من أجل منع استغلالها لأغراض انتهاك قرارات مجلس الأمن وبإبلاغ السلطات المختصّة كما هو واجب عن أي (محاولة) التفاف على العقوبات.

تمويل الإرهاب

تشمل عبارة تمويل الإرهاب تزويد الأموال من أجل ارتكاب أنشطة إرهابية ودعم الشخص الإرهابي أو المجموعة الإرهابية. ويشمل ذلك تزويد المأكل والمأوى والتدريب وتوفير الوسائل مثل النقل ومعدّات الاتصال. ويمكن لهذا التمويل أن يتم عبر المال أو بمساعدة عينية ويمكن للأموال المستخدمة أن تأتي من مصادر مشروعة أو غير مشروعة.

إنّ المعلومات التالية هي عبارة عن طرُق وحالات تظهر كيف قامت المجموعات الإرهابية باستغلال القطاعات أو الأنشطة المالية من أجل تمويل أنشطتها. ويجمع هذا المستند المعلومات من مستندات طوّرها مجلس الأمن ومكتب الأمم المتحدة المعني بالمخدرات والجريمة ومجموعة العمل المالي (الفاتف).

طرق تمويل الإرهاب

حددت الفاتف في تقريرها تحت عنوان "تمويل تنظيم داعش الإرهابي" الصادر عام 2015 أنّ ذلك التنظيم الإرهابي يجني المداخيل من 5 مصادر أساسية: (1) المتحصلات غير المشروعة من جراء احتلال الأراضي، مثل نهب البنوك والابتزاز والسيطرة على حقول ومصافي النفط وسرقة الأصول الاقتصادية وفرض الضرائب غير المشروعة على السلع والنقد الذي يعبر الأراضي التي ينشط فيها التنظيم؛ (2) الخطف مقابل فدية؛ (3) التبرعات بما فيها التبرعات من قبل المنظّمات غير الربحية أو من خلالها؛ (4) الدعم المادي كالدعم المرتبط بالمقاتلين الإرهابيين الأجانب و(5) جمع الأموال من خلال شبكات التواصل العصرية[1].

وبحسب استنتاج الاستبيان الذي أرسل إلى كافة الدول الأعضاء في الأمم المتحدة والوراد في التقرير المشترك للمديرية التنفيذية للجنة مكافحة الإرهاب وفريق الدعم التحليلي ورصد الجزاءات العامل بموجب القرارين 1526 (2004) و2253 (2015) بشأن تنظيم الدولة الإسلامية في العراق والشام (داعش) وتنظيم القاعدة وحركة طالبان وما يرتبط بها من أفراد وكيانات عن الإجراءات التي اتخذتها الدول الأعضاء لوقف تمويل الإرهاب، الذي أعدّ عملاً بالفقرة 37 من قرار مجلس الأمن 2462 (2019) بتاريخ 3 يونيو 2020 ("التقرير المشترك")، إنّ القنوات الأكثر استخداماً لتمويل الإرهاب هي (1) النظام المصرفي الرسمي؛ (2) تهريب النقد؛ (3) شركات الخدمات المالية؛ و(4) دور الحوالة غير الرسمية[2].

يشير التقرير المشترك أيضاً إلى إساءة استخدام التكنولوجيا (بما في ذلك وسائل التواصل الاجتماعي والبطاقات مسبقة الدفع والعمليات المصرفية عبر الأجهزة المحمولة) لأغراض إرهابية، مع الإشارة إلى تيسير تمويل الإرهاب بفعل التطورات الحديثة في الدفع بواسطة الأجهزة المحمولة وعدم الكشف عن الهوية في التحويلات المالية والتبرّعات غير المشروعة من خلال منصات التمويل الجماعي.[3]

---

[1] مجموعة العمل المالي (فاتف)، 2015، ص. 12

[2] المديرية التنفيذية للجنة مكافحة الإرهاب وفريق الدعم التحليلي ورصد الجزاءات العامل بموجب القرارين 1526 (2004) و2253 (2015)، S/2020/493، ص. 19

[3] المديرية التنفيذية للجنة مكافحة الإرهاب وفريق الدعم التحليلي ورصد الجزاءات العامل بموجب القرارين 1526 (2004) و2253 (2015)، S/2020/493، ص. 20

ويلاحظ مجلس الأمن التابع للأمم المتحدة أنّ الإرهابيين والجماعات الإرهابية يجمعون الأموال من خلال وسائل متنوعة، منها استغلال الموارد الطبيعية والخطف طلباً للفدية والصلات القائمة بالجريمة المنظمة والاتجار بالمخدرات. ويشير التقرير المشترك إلى إمكانية تمويل الإرهاب من خلال قطاعي البناء والعقارات واستخدام الشركات الوهمية لإخفاء الأموال النقدية واستخدام المنظمات غير الربحية وتمويل الإرهاب القائم على التجارة[4].

الأساليب الأكثر استخداماً من قبل الجهات المموّلة للإرهاب

المصدر: المديرية التنفيذية للجنة مكافحة الإرهاب وفريق الدعم التحليلي ورصد الجزاءات العامل بموجب القرارين 1526 (2004) و2253 (2015)، S/2020/493، ص. 19.

الخدمات المصرفية

يُعتبر النظام المصرفي معرّضاً لخطر تمويل الإرهاب بسبب صعوبة التمييز بين المعاملات المشروعة والمعاملات غير المشروعة المنخفضة التكلفة ورصد المعاملات غير المباشرة. وفي الكثير من الأحيان تعجز برامج رصد المعاملات عن الكشف عن تمويل الإرهاب. كما يظهر خطر استخدام القروض المصرفية والاستحقاقات الاجتماعية المدفوعة من خلال المصارف لتمويل الإرهاب[5].

---

[4] المديرية التنفيذية للجنة مكافحة الإرهاب وفريق الدعم التحليلي ورصد الجزاءات العامل بموجب القرارين 1526 (2004) و2253 (2015)، S/2020/493، ص. 20

[5] المديرية التنفيذية للجنة مكافحة الإرهاب وفريق الدعم التحليلي ورصد الجزاءات العامل بموجب القرارين 1526 (2004) و2253 (2015)، S/2020/493، ص. 19

النفاذ المستمرّ للحسابات المصرفية من قبل المقاتلين الإرهابيين الأجانب

وبحسب بعض المعلومات المالية الحسّاسة، تمّ اكتشاف مخاطر تمويل إرهاب متعلّقة بالسحوبات النقدية عبر آلات سحب الأموال في الخارج والتي تمّت في مناطق قريبة من الأراضي التي ينشط فيها تنظيم داعش من قبل أشخاص غير معروفين. وقد تمت هذه السحوبات من حسابات مصرفية موجودة في الولايات المتحدة باستخدام بطاقات مدينة (Debit card). كما تمّ تحديد خطر تمويل إرهاب آخر في وجود إيداعات كبيرة في الحسابات المصرفية تليها فوراً سحوبات نقدية في الخارج في مناطق قريبة من الأراضي التي ينشط فيها تنظيم داعش. وتكشف هذه المعلومات عن مخاطر تمويل الإرهاب التي تشكّلها القدرة المستمرّة للأفراد الذين يُعتقد بأنهم سافروا إلى المناطق المحتلة من قبل داعش على النفاذ إلى حساباتهم المصرفية في بلدانهم الأم. المصدر: الولايات المتحدة[6].

محوِّلو الأموال

إلى جانب النظام المصرفي، تمت إساءة استخدام قطاع تحويل الأموال من أجل نقل الأموال غير المشروعة وهو أيضاً عرضة لتمويل الإرهاب. ففي الدول التي يكون فيها الوصول إلى الخدمات المصرفية محدوداً، قد يصبح مزوّدو خدمات التحويل المؤسسة المالية الأساسية التي يتعامل معها المستهلك للقيام بأنشطة تحويل الأموال عبر الحدود. ويتعرّض مزوّدو خدمات التحويل لمخاطر الاستغلال لتمويل الإرهاب بشكلٍ خاص عندما لا يخضعون للتنظيم أو الرقابة المناسبة لجهة مكافحة غسل الأموال وتمويل الإرهاب أو حيث يعملون من دون ترخيص (وبالتالي يعملون من دون أي ضوابط لمكافحة غسل الأموال أو تمويل الإرهاب)[7].

تواطؤ أحد الموظفين لدى مؤسسة تزوّد خدمات تحويل القيمة المالية

تمكّن أحد الأفراد من جمع الأموال لمنظّمة الشباب من الجالية الصومالية في ولاية ميسوري الأميركية وغيرها من المناطق واستخدم مجموعة من شركات الخدمات المالية المرخّصة التي لديها مكاتب في الولايات المتحدة من أجل تحويل الأموال إلى الصومال لدعم مقاتلي الشباب بشكلٍ عام. وقد ساعد هذا الشخص أحد المتواطئين الذي كان يعمل لدى إحدى شركات الخدمات المالية المتورّطة لتفادي أي أثر ورقي للمعاملات عبر هيكلتها على مبالغ صغيرة بالدولار واستخدام معلومات كاذبة لتحديد الهوية. وقد استخدم الموظّف لدى شركة الخدمات المالية وغيره من المتواطئين أسماء وأرقام هاتفية وهمية لإخفاء طبيعة معاملاتهم[8].

دور الحوالة وغيرها من مزوّدي الخدمات الشبيهة

هناك عدة أسباب خلف تشكيل دور الحوالة وغيرها من مزوّدي الخدمات الشبيهة نقطة ضعف من حيث تمويل الإرهاب، بما في ذلك: عدم التسجيل والرقابة والسداد عبر عدة بلدان من خلال القيمة أو النقد خارج النظام المصرفي في بعض الحالات

[6] مجموعة العمل المالي (فاتف)، فبراير 2015، ص. 23
[7] مجموعة العمل المالي (الفاتف)، أكتوبر 2015، ص. 26
[8] مجموعة العمل المالي (الفاتف)، أكتوبر 2015، ص. 26

واستخدام الأعمال التي تشكّل مؤسسات مالية غير منظّمة واستخدام التسوية الصافية واختلاط المتحصلات المشروعة مع تلك غير المشروعة[9].

استغلال الإرهابيين لدور الحوالة وغيرها من مزوّدي الخدمات الشبيهة

تمّ اعتراض مبلغ 10،000،000 روبية هندية (160،000 دولار أميركي) في الولاية أ في الهند كان من المنوي تسليمه للمجموعة الإرهابية X. وأظهر التحقيق أن عدداً من الشحنات السابقة تم تسليمها للمجموعة الإرهابية في وقتٍ سابق. وتم الكشف عن اختلاس صناديق تنمية في منطقة محددة في تلك الولاية ثم أرسلت إلى الموقع ب في تلك الولاية ومن الموقع ب تم إرسال الأموال إلى الموقع ك في ولاية أخرى (الولاية ب) بمساعدة عاملي حوالة (Hundi) يعملون بين الولاية أ والولاية ب. يُقال لمشغلي دور الحوالة أنّ الأموال تعود لشخص نافذ جداً في الولاية أ ولا يعترض هؤلاء على إجراء المعاملة لدى سماع اسم ذلك الشخص النافذ ويسلّمون الأموال في الولاية ب إلى الشخص المخوّل من قبل ممثل المجموعة الإرهابية. يتم تسليم الأموال بعد خصم عمولة بقيمة 1 في المئة من المبلغ الإجمالي الذي يتم تحويله. في الولاية ب، يتم تحويل أموال الحوالة من الروبية إلى الدولار بسوق الصرافة غير المنظّم ثم تحويلها إلى دولة أخرى حيث يتم شراء الأسلحة والذخيرة من قبل قادة المجموعة الإرهابية المتمركزين هناك. ثم يتم نقل تلك الأسلحة والذخائر عبر الحدود وتسليمها إلى المجموعة الإرهابية الناشطة في الولاية أ للقيام بأنشطتها الإرهابية. وفي هذه القضية تمّ إلقاء القبض على 15 متهماً وتوجيه التهم إليهم وتتم المحاكمة حالياً. ويشمل الأعضاء الذين تم إلقاء القبض عليهم إرهابيين ومتعاقدين ووكلاء وموظّفين حكوميين[10].

تسهيلات الدفع عبر الإنترنت

تسهّل تسهيلات الدفع عبر الإنترنت المقدّمة من خلال المواقع الإلكترونية المخصصة أو منصات التواصل عملية نقل الأموال بشكلٍ إلكتروني بين الأطراف. فيتمّ تحويل الأموال بأغلب الأحيان بواسطة التحويلات البرقية الإلكترونية أو البطاقات الائتمانية أو تسهيلات الدفع الأخرى المتوفرة عبر خدمات مثل PayPal أو Skype[11].

جمع التبرعات عبر الإنترنت

تشير المعلومات الاستخبارية إلى أنّ بعض الأفراد المرتبطين بتنظيم داعش قد دعوا الأشخاص للتبرّع من خلال منصّة تويتر وطلبوا من المتبرّعين الاتصال بهم عبر تطبيق سكايب (Skype). وفي هذا الإطار يُطلَب من المتبرّعين شراء بطاقة دولية مسبقة الدفع (مثل بطاقة شحن رصيد لخطّ هاتف نقّال أو شراء تطبيق أو أي برنامج آخر يسمح بتخزين الرصيد) وإرسال رقم البطاقة مسبقة الدفع عبر تطبيق سكايب. بعد ذلك يقوم الشخص الذي يجمع الأموال بإرسال الرقم إلى أحد أتباعه في إحدى الدول القريبة من سوريا ويبيع رقم البطاقة بسعر أدنى ويأخذ النقود ويعطيها في وقتٍ لاحق لتنظيم داعش. المصدر: المملكة العربية السعودية[12].

---

[9] مجموعة العمل المالي (الفاتف)، أكتوبر 2013، ص. 41
[10] مجموعة العمل المالي (الفاتف)، أكتوبر 2013، ص. 43
[11] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2012، ص. 7
[12] مجموعة العمل المالي، فبراير 2015، ص. 24-25

استخدام حسابات PayPal لجمع الأموال

كانت إحدى المؤسسات الخيرية التي تم إنشاؤها عام 2000 والتي يتخصص رئيسها في التسويق الإلكتروني تعرض على موقعها الإلكتروني عدة خيارات للتبرّع عبر البطاقات الائتمانية أو نظام PayPal أو التحويلات النقدية أو الشيكات. وخلال سنة ونصف، تلقّت الحسابات المصرفية الخاصة بتلك المؤسسة الخيرية تبرّعات عديدة على شكل شيكات وتحويلات برقية تحت مبلغ 500 يورو. ومن أصل مبلغ 2 مليون يورو الذي تم جمعه، أتى مبلغ 600،000 يورو من بضع عمليات عبر منصة PayPal من دولة أخرى. كما تم استخدام حسابات شخصية على PayPal ايضاً من أجل جمع الأموال ليتم سحبها لاحقاً بشكلٍ نقدي أو تحويلها إلى حسابات أخرى. المصدر: فرنسا[13].

السرقة من خلال تسهيلات الدفع عبر الإنترنت

يمكن أن تكون تسهيلات الدفع عبر الإنترنت عرضةً لانتحال الشخصية وسرقة البطاقة الائتمانية والاحتيال الالكتروني والاحتيال في الأوراق المالية والجرائم الخاصة بالملكية الفكرية والاحتيال في المزادات.

قضية المملكة المتحدة ضد يونس التسولي: تمّ غسل الأرباح الناتجة عن سرقة بطاقات ائتمانية بواسطة وسائل مختلفة، بما في ذلك التحويل عبر حسابات دفع الذهب الإلكتروني (e-gold) التي استُخدمت من أجل تحويل الأموال عبر دول عديدة قبل وصولها إلى الوجهة المنشودة. وقد تم استخدام الأموال المغسولة من أجل تمويل تسجيل 180 موقع إلكتروني من قبل التسولي لاستضافة فيديوهات من ضمن الترويج لتنظيم القاعدة وأيضاً لتزويد المعدات لأنشطة إرهابية في عدة دول. وقد تم استخدام نحو 1400 بطاقة ائتمانية للحصول على ما يقارب 1.6 مليون جينيه استريليني من الأموال غير المشروعة لتمويل أنشطة إرهابية[14].

التبرعات من قبل المنظمات غير الربحية أو من خلالها

قد يحاول البعض من الأفراد والتنظيمات الذين يسعون إلى جمع الأموال لدعم الإرهاب والتطرف إخفاء أنشطتهم عبر الادعاء بأنهم يشاركون في أنشطة خيرية أو إنسانية وقد يؤسسون المنظمات غير الربحية لهذه الأغراض[15].

تحويل الأموال من قبل عاملين لدى المنظمات غير الربحية

أسس أحد الأشخاص (السيد أ) مؤسسة خيرية تحت حجّة جمع التبرعات للاجئين السوريين والأشخاص المحتاجين للمساعدة الطبية والمالية وبناء المساجد والمدارس ورياض الأطفال. إلا أنّه في الحقيقة كان السيد أ يقود مخططاً منظّماً لإرسال التبرعات إلى مجموعة من الأفراد المرتبطين بالسيد أ بدل حساب المؤسسة. وفي أكثرية الحالات، تُرسل الأموال في المرحلة الأولى من خلال محوّلي الأموال ثم تنقل بشكلٍ نقدي. بعد ذلك، تحول الأموال إما إلى حسابات بطاقات ائتمانية أو إلى محفظات إلكترونية. وقد وضع أعضاء المجموعة أ المعلومات ذات الصلة (التي تفيد بأن الأموال تُجمع من أجل الأهداف

---

[13] مجموعة العمل المالي، فبراير 2015، ص. 38
[14] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2012، ص. 7
[15] مجموعة العمل المالي، أكتوبر 2015، ص. 32

المعلنة) على الإنترنت ولكن كانت هذه الأموال تُرسل في الواقع كمساعدة لإرهابيين وعائلاتهم وكان من المنوي استخدامها كدعم مالي للأنشطة الإرهابية. تم اكتشاف هذه المعلومات من خلال تحقيقات قامت بها وحدة المعلومات المالية بناءً على المراقبة الدورية للكيانات على لائحتها المحلية من الكيانات الإرهابية المدرجة والأشخاص المتربطين بهم أو بناءً على معلومات من جهات إنفاذ القانون. وقد سمح تحليل المعلومات للوحدة أن تحدد العلاقة بين القضايا المختلفة: متبرّعون ومتلقّون مشتركون وطريقة عمل شبيهة لجمع الأموال وتوزيعها. سمح المزيد من التعاون مع سلطات إنفاذ القانون للوحدة أن تكتشف الرابط المباشر بين السيد أ ونشاط داعش. وقد أدى ذلك إلى عدة تحقيقات جنائية مرتبطة بالسيد أ. كما أنّه تم إدراج السيد أ على القائمة المحلية للكيانات الإرهابية مع اتخاذ تدابير التجميد ذات الصلة. وقد تم تجميد أصول أعضاء المجموعة أ، بموجب أوامر صادرة عن المحكمة[16].

تهريب الأموال النقدية

ما زالت الأموال النقدية تشكّل وجهاً أساسياً من العمليات الإرهابية وفيما قد يتم جمع الأموال بطرق مختلفة، إلا أنّها غالباً ما تحوّل إلى أموال نقدية لتُنقل إلى مناطق النزاع. وتساعد في ذلك الحدود الوطنية غير المضبوطة وصعوبة رصد عمليات تهريب النقد (خاصة المبالغ الصغيرة التي يتم أحياناً تهريبها لأغراض تمويل الإرهاب)، ووجود الاقتصادات غير الرسمية وغير المنظّمة[17].

ناقلو النقد

طوال فترة ثلاثة أيام متتالية قام ثلاثة أفراد بالإقرار عن مبلغ أجمالي يصل إلى حوالي 90،000 يورو نقداً لمسؤولي الجمارك في مطار بروكسيل. وقيل أنّ الأموال مصدرها المنظمة غير الربحية "أ" من ألمانيا كجزءٍ من المساعدات الإنسانية في بوروندي ودولة بينين وزمبابوي. وكان ناقلو النقد الثلاثة من الجنسية البلجيكية ويعيشون في بلجيكا منذ فترة طويلة ويمتلكون الحسابات. وكانت جهة تنسيق بلجيكية لمنظمة إسلامية متطرّفة تحوّل الأموال لهذه الحسابات. وخلال فترة سنة واحدة تم سحب مبلغ يقارب 20،000 يورو. وقد تم تحويل نحو 10،000 يورو إلى تركيا. وبحسب وحدة المعلومات المالية الألمانية، كانت المنظمة غير الربحية "أ" من أكبر المنظمات الإسلامية في ألمانيا ويُقال إنها مرتبطة بالمنظمة غير الربحية "ب" التي تم حظرها في ألمانيا لدعمها منظمة إرهابية. كما كان كافة أعضاء مجلس إدارة المنظّمة "ب" يضطلعون بدور أساسي في المنظمة غير الربحية "أ".

وبحسب المعلومات من أجهزة الاستخبارات البلجيكية من المعروف عن الأفراد الثلاثة المذكورين آنفاً أنهم مرتبطون بفروع محلية لمنظمة إسلامية متطرفة. ونظراً لطبيعة المعاملات والروابط بين المنظمتين المذكورتين أعلاه، تشكّ السلطات البلجيكية في أن يكون قد استُخدم على الأقل جزء من الأموال المذكورة أعلاه لدعم أنشطة إرهابية[18].

---

[16] مجموعة العمل المالي، فبراير 2015، ص.20

[17] مجموعة العمل المالي، أكتوبر 2015، ص. 23

[18] مجموعة العمل المالي، أكتوبر 2015، ص. 23

تمويل انتشار أسلحة الدمار الشامل

إنّ عبارة انتشار أسلحة الدمار الشامل ليست محدودة بتزويد أو إتاحة المواد أو المعدات الكيميائية أو البيولوجية أو الإشعاعية أو النووية من أجل صنع الأسلحة، بل تشمل أيضاً نقل وتصدير التكنولوجيا أو السلع أو البرمجيات أو الخدمة أو الدراية التي يمكن استخدامها في البرامج المرتبطة بالأسلحة النووية أو الكيميائية أو البيولوجية.

وبالتالي، إنّ تمويل الانتشار هو تزويد الخدمات المالية لتلك البرامج من أجل نقل وتصدير الأسلحة النووية أو الكيميائية أو البيولوجية وقنوات تسليمها والمواد المرتبطة بها. كما يشمل تمويل الانتشار أيضاً تمويل التجارة بالسلع الحسّاسة المطلوبة لدعم تلك البرامج أو الحفاظ عليها، حتى لو لم تكن تلك السلع مرتبطة بأي مواد نووية أو كيميائية أو بيولوجية، مثل النفط والفحم والحديد ومعدات الاتصال العسكرية. بالإضافة إلى ذلك، يشمل تمويل الانتشار الدعم المالي للأفراد أو الكيانات المشاركة في الانتشار حتى لو كانوا يمارسون أنشطة أخرى غير مرتبطة بتلك البرامج مثل: الدبلوماسيين وشركات الشحن أو مصايد السمك وشركات التجارة بالسلع.

تظهر الحالات التالية قضايا مخالفة للعقوبات المفروضة من قبل مجلس الأمن والمرتبطة بالبرنامج النووي لجمهورية كوريا الشعبية الديموقراطية أو التهرب منه، كما عرضها فريق الخبراء المنشأ بموجب القرار 1874، بين عامي 2017 و2020 ("فريق الخبراء").

تشمل القضايا الموضحة أدناه عدة قطاعات على الصعيد العالمي بما في ذلك القطاع المالي وقطاعي التجارة والشحن وتدلّ على حاجة الدول لزيادة الوعي في كافة القطاعات الاقتصادية حول هذه العقوبات وأهمية تطبيقها.

في ما يتعلّق بإيران، فقد تبنّى القرار 2231 بتاريخ 20 يوليو، 2015 خطة العمل الشاملة المشتركة (JCPOA) التي تم التفاوض عليها بين إيران وأعضاء مجلس الأمن الدائمين الخمسة زائد واحد (الصين وفرنسا وروسيا والمملكة المتحدة والولايات المتحدة زائد ألمانيا)، ما خفّف بشكلٍ كبير برنامج العقوبات المرتبطة بالبرنامج النووي الإيراني. وتركّز عملية التحقق حالياً بشكلٍ أكبر على النشاط النووي بحدّ ذاته وتقوم بها المنظمة الدولية للطاقة الذرية، وبالتالي فهي مسألة غير ذات صلة بالنسبة إلى هذا المستند.

التدابير المالية

الأصول المالية

الأنشطة المالية للدبلوماسيين وغيرهم من الموظفين التابعين لجمهورية كوريا الشعبية الديمقراطية

حقق فريق الخبراء في أمر الموظفين الدبلوماسيين أو الرسميين التابعين لجمهورية كوريا الشعبية الديمقراطية الذين يتصرفون باسم مؤسسات مالية خاضعة للجزاءات بغرض إنشاء شبكات مصرفية غير مشروعة وإتاحة إمكانية الاستفادة من النظم المصرفية العالمية.

وحقق فريق الخبراء في تقارير تفيد بأن جو كوانغ تشول، وهو أحد الأعضاء المعتمدين من الموظفين الإداريين والتقنيين في سفارة جمهورية كوريا الشعبية الديمقراطية في النمسا منذ عام 2016، قد شارك في أنشطة للتهرب من الجزاءات باسم

مصـــرف Foreign Trade Bank المدرج في قائمة الجزاءات. ووفقاً للمعلومات التي قدمتها النمسا، حاول السيد جو الوصول إلى الحسابات المجمدة لشركة Korea Ungum Corporation في أحد المصـــارف النمســـاويـة. وقد جمدت السـلطات النمسـاوية حسـابات الشـركة في يوليو 2015 بسـبب الاشـتباه في قيامها بأنشـطة غسـل أموال. وفي ذلك الوقت، كان الرصـيد الإجمالي للشـركة حوالي 1،895،633 دولاراً.

الأنشطة الإلكترونية التي تستهدف المؤسسات المالية

تتوفّر الأدلّة التي تفيد بأنّ جمهورية كوريا الشعبية الديموقراطية تستخدم الهجمات الإلكترونية لسرقة الأموال من المؤسسات المالية وبورصات العملات المشفّرة في دول مختلفة ما يسمح لهذه الدولة بالتهرب من الجزاءات المالية وتوليد الإيرادات بطرق يصعب تعقّبها وتخضع لنسبة أقلّ من الرقابة والتنظيم الحكوميين. خلال عام 2019، جرت تحقيقات في 35 حالة مبلّغ عنها على الأقل لتنفيذ جهات فاعلة من جمهورية كوريا الشـعبية الديمقراطية بمهاجمة مؤسـسـات مالية، وبورصـات للعملات المشفّرة، وأنشطة تعدين ترمي إلى كسب عملات أجنبية، بما في ذلك الدول الأعضـاء التالية: بنغلادش (حالتان)، وبولندا (1)، وتونس (1)، وجمهورية كوريا (10)، وجنوب أفريقيا (1)، وسلوفينيا (1)، وشيلي (2)، وغامبيا (1) وغواتيمالا (1)، وفييت نام (1)، وكوستاريكا (1)، والكويت (1)، وليبريا (1)، ومالطة (1)، وماليزيا (1)، ونيجيريا (1)، والهند (3)[19].

وبحسب تقرير فريق الخبراء المنشأ بموجب قرار مجلس الأمن 1874 S/2019/691، تبيّن التحقيقات أنّه منذ العام 2019 حصلت زيادة ملحوظة في نطاق وبراعة تلك الأنشطة الجارية الإلكترونية. وأشارت بعض التقديرات إلى أنّ المبلغ الذي اكتسبته جمهورية كوريا الشعبية الديمقراطية بصورة غير مشروعة يصل إلى بليونَي دولار[20].

عملية "FASTCash"

أشار فريف الخبراء في تقريره لأغسطس 2019 إلى إحدى الهجمات الإلكترونية التي قامت بها جهات فاعلة في جمهورية كوريا الشعبية الديمقراطية من الوصول إلى الهياكل الأساسية التي تدير كامل شبكات آلات صرف الأموال في إحدى الدول الأعضاء لأغراض تركيب برمجيات حاسوبية خبيثة تعدّل تجهيز المعاملات من أجل القيام عنوةً بـــ 10 000 عملية لتوزيع الأموال النقدية على أفراد يعملون لصالح جمهورية كوريا الشعبية الديمقراطية أو نيابة عنها في أكثر من 20 بلدا في ظرف خمس ساعات. وتطلبت هذه العملية أعداداً كبيرة من الأشخاص في الميدان، مما يشـير إلى تنسـيق واسـع النطاق مع رعايا جمهورية كوريا الشـعبية الديمقراطية العاملين في الخارج وإمكانية التعاون مع شبكة الجريمة المنظّمة[21].

وقد تمّ تمكين العملية المعروفة تحت إسم "FASTCash" من قبل مجموعة لازاروس المعروفة بتورّطها في الهجمات الإلكترونية والأنشطة الجاسوسية، مع روابط واضحة بجمهورية كوريا الديمقراطية الشعبية. وسمحت هذه العملية بإفراغ آلات صرف الأموال من النقود عبر الاحتيال. ومن أجل القيام بتلك السحوبات النقدية غير المشروعة، قامت مجموعة لازاروس أولاً بقرصنة شبكات البنوك المستهدفة واخترقت خوادم التطبيق الذي يدير العمليات على آلات صرف الأموال.

---

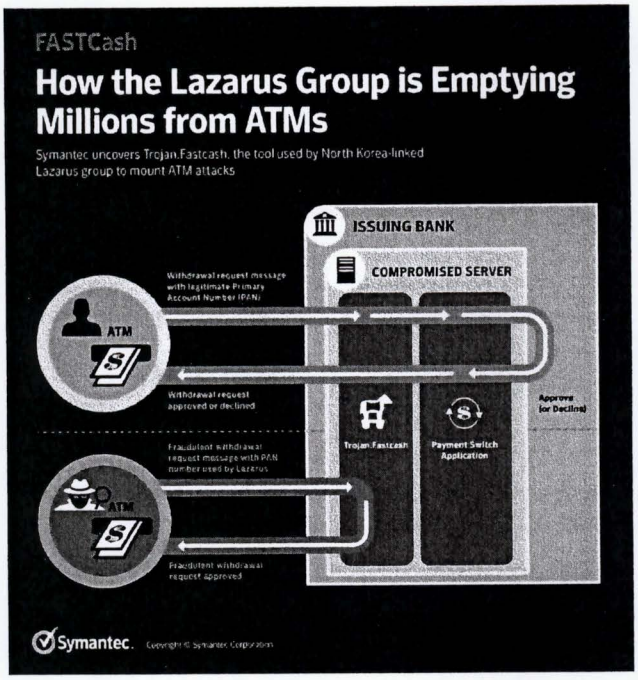
[19] تقرير فريق الخبراء المنشأ بموجب قرار مجلس الأمن 1874، S/2019/691، ص. 29

[20] تقرير فريق الخبراء المنشأ بموجب قرار مجلس الأمن 1874، S/2019/691، ص. 29

[21] تقرير فريق الخبراء المنشأ بموجب قرار مجلس الأمن 1874، S/2019/691، ص. 29

متى تمّ اختراق تلك الخوادم، تمّ إطلاق البرنامج الحاسوبي الخبيث (Trojan.Fastcash) الذي لم يكن معروفاً بعد من أجل اختراق طلبات سحب النقود المبنية على الاحتيال من قبل مجموعة لازاروس وإرسال موافقات مزيّفة على العمليات ما سمح للمعتدين أن يسرقوا النقود من آلات صرف الأموال.

وبحسب إحدى الإنذارات الصادرة عن الحكومة الأميركية، تمّ سحب النقود بالتزامن من آلات صرف الأموال في أكثر من 30 دولة مختلفة في حادثة واحدة عام 2017. وفي حادثة كبرى أخرى حصلت عام 2018، تم سحب النقود من آلات صرف الأموال في 23 دولة مختلفة. وحتى اليوم، يُقدّر أنّ عملية FASTCash التي قامت بها مجموعة لازاروس قد أدت إلى سرقة عشرات الملايين من الدولارات[22].



المصدر: "FASTCash: How the Lazarus Group is emptying millions from ATMs", Symantec, 2 October 2018. Available at www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware.

الهجمات الإلكترونية على بورصات العملات المشفّرة

عام 2019، تحوّل اهتمام الجهات الفاعلة في الفضاء الإلكتروني في جمهورية كوريا الشعبية الديمقراطية، إلى استهداف بورصات العملات المشفّرة. وهوجم بعض بورصات العملات المشفرة عدة مرات، وخاصةً تلك المسجّلة في جمهورية كوريا. فقد تعرضت بورصة bithumb للعملات المشفّرة للهجوم من جهات فاعلة في جمهورية كوريا الشعبية الديمقراطية أربع مرات على الأقل. وأسفر كل من الهجومين الأول والثاني في فبراير ويوليو 2017 عن خسائر تناهز 7 ملايين دولار، في حين أسفر هجومان لاحقان في يونيو 2018 ومارس 2019 عن خسارة 31 مليون و20 مليون دولار، على التوالي،

[22] FASTCash: How the Lazarus Group is emptying millions from ATMs, Symantec, 2 October 2018. Available at www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware.

مما يدل على زيادة في قدرة الجهات الفاعلة في جمهورية كوريا الشعبية الديمقراطية وفي تصميمها. وكذلك، تعرضت بورصة Youbit (Yapizon سابقاً) لهجمات متعددة أسفرت عن خسارة 4.8 ملايين دولار في أبريل 2017 ثم 17 في المائة من إجمالي أصولها في ديسمبر 2017، مما أجبر البورصة على الإغلاق[23].

احتفاظ البنوك المدرجة بمكاتب تمثيلية ووكلاء في الخارج

أشار فريق الخبراء في فبراير 2017 أنّه حصل على معلومات تبيّن أن ثمة مصرفين مدرجين، هما Daedong Credit Bank (DCB) و Korea Daesong Bank (KDB)، يعملان على الأراضي الصينية، عن طريق مكاتب تمثيلية في داليان وداندونغ وشينيانغ. وقد شغل أحد مدراء هذه المكاتب أيضاً منصب مدير شركة مدرجة، DCB Finance Ltd المسجلة في جزر فرجن البريطانية. وتشاركت شركة DCB Finance عدة موظفين مع مصرف DCB. عندما أغلقت الحسابات المراسلة لمصرف DCB في عام 2005، أنشئت شركة DCB Finance لإجراء التحويلات البرقية والمعاملات التجارية باسمه[24].

وقد أجرى ممثل مصرف DCB وشركة DCB Finance في داليان، معاملات بملايين الدولارات، منها عدة معاملات بلغت قيمة كل منها مليون دولار أو أكثر. ويسّر أيضاً مدفوعات وقروض بين مختلف الشركات المرتبطة بمصرف DCB وقام بتبديل كميات كبيرة من المبالغ النقدية المحولة إلى الصين من جمهورية كوريا الشعبية الديمقراطية إلى أوراق نقدية بعملة دولار أميركي أحدث أو ذات فئة أكبر. وأجرى كذلك معاملات تصريف في سوق الصرف الأجنبي بين الدولار واليورو وحوّل أرصدة بين مصرف DCB والمصرف المساهم فيه، Korea Daesong Bank. وعندما أنشأ مصرف DCB مكاتب تمثيلية في شينيانغ في أواخر عام 2012، وداندونغ في عام 2014، تعاونت المكاتب الثلاثة في إدارة أنشطة الصرف الأجنبي، والتحويل، وتبادل المبالغ النقدية الضخمة، والقروض[25].

الموارد الاقتصادية

المبالغ النقدية والذهب

يتم استخدام المبالغ النقدية الضخمة والذهب من قبل جمهورية كوريا الديمقراطية الشعبية لنقل القيمة عبر تفادي القطاع المالي الرسمي برمّته. والحالات التالية هي بعض الحالات التي رصدها تقرير فريق الخبراء.

في 6 مارس 2015، ضبطت بنغلاديش 26.7 كيلوغراماً من سبائك الذهب والمجوهرات (بقيمة 1.4 مليون دولار) كانت في الأمتعة المحمولة للسكرتير الأول لسفارة جمهورية كوريا الشعبية الديمقراطية في داكا. وقد صدرت الفاتورة المرتبطة بتلك السلع عن شركة AMM Middle East General Trading في دبي وجرى تحصيل البضاعة في سنغافورة. وقد سافر السكرتير الأول من داكا إلى سنغافورة وغادرها في اليوم نفسه، وخرج من المطار لمدة ثلاث ساعات. وكان قد قام برحلات من هذا القبيل بمتوسط مرة في الشهر إلى سنغافورة على مدى الأشهر الخمسة عشر السابقة منطلقاً من داكا ومن بيجين

[23] تقرير فريق الخبراء المنشأ بموجب قرار مجلس الأمن 1874، S/2019/691، ص. 31
[24] تقرير فريق الخبراء بموجب قرار مجلس الأمن 1874، S/2017/150K، ص. 95
[25] تقرير فريق الخبراء بموجب قرار مجلس الأمن 1874، S/2017/150K، ص. 96

(كان يقضي فترة تتراوح بين بضع ساعات ويومين خارج المطار)، مما يوحي بأنه كان يؤدي دور حامل الحقيبة الدبلوماسية الدائم ويهرّب الذهب وأصنافاً أخرى للتهرب من الجزاءات. وكان يرافقه في بعض من هذه الرحلات دبلوماسيون آخرون من جمهورية كوريا الشعبية الديمقراطية[26].

وفي 17 مارس 2016، أُلقِيَ القبض في مطار كولومبو في سري لانكا على شخص من جمهورية كوريا الشعبية الديمقراطية يعمل في الخارج، كان يحمل مبلغ 000 167 دولار من النقد والمجوهرات الذهبية والساعات. وكان في طريقه من سلطنة عُمان إلى بيجين ولم يقدم تصريحاً جمركياً. وكان يرافقه خمسة أفراد آخرين من جمهورية كوريا الشعبية الديمقراطية يعملون في عُمان في شركة بناء تابعة لجمهورية كوريا الشعبية الديمقراطية ومقرها في دبي وتملك عنوان صندوق بريد. وأعدّ قائمة تتضمن 311 اسماً لعمال من جمهورية كوريا الشعبية الديمقراطية تعيش أسرهم في بيونغ يانغ كان عليه أن يدفع لها المال (يُدفَع لكل أسرة مبلغاً يتراوح بين 200 و1500 دولار، بمتوسط 300 دولار للأسرة الواحدة)[27].

عمليات نقل النفط من سفينة إلى أخرى

استحصل فريق الخبراء منذ العام 2018 على أدلّة تشير إلى تزايد وتيرة نقل النفط من سفينة إلى أخرى ولعملية نقل ممنوعة غير مسبوقة لمنتج نفطي شملت 57،623.491 برميل نفط تساوي قيمتها 5،730،886 دولار. وتشير تحقيقات الفريق حول عملية النقل هذه قضية معقّدة جداً للاحتيال في هوية السفن مرتبطة بجمهورية كوريا الديمقراطية الشعبية، تسلّط الضوء على تقنيات جديدة للتهرب من العقوبات تغلّبت على جهود العناية الواجبة لأحد تجار السلع الأبرز في المنطقة بالإضافة إلى البنوك الأميركية والسنغافورية التي سهّلت دفعات الوقود وإحدى جهات التأمين البارزة البريطانية التي أمّنت الحماية والتأمين لإحدى السفن المتورّطة. وتشير القضية أيضاً مرة أخرى إلى رداءة عملية رفع التقارير والرقابة والضبط على السفن التي تمارسها الدول التي تبحر تلك السفن تحت علَمها[28] بالإضافة إلى التقصير في تطبيق عقوبات التجميد.

قضية سفينة Lighthouse Winmore

حقق فريق الخبراء في أربع سفن ضالعة في انتهاك الفقرتين ١١ و١٤ من القرار 2375 (2017). وفي حين أن مقر شبكتها يوجد أساساً في مقاطعة تايوان الصينية، فقد سُجِّلت شركاتها في ولايات قضائية متعددة، تشمل جزر فرجن البريطانية وجزر مارشال وساموا وسيشيل وهونغ كونغ، وترفع السفن أعلام بنما ودومينيكا وسيراليون وهونغ كونغ.

وقد قامت أول ناقلتي نفط حقق بشأنهما الفريق، وهما الناقلة *Lighthouse Winmore* التي ترفع علم هونغ كونغ، والناقلة *Billions No.18* التي ترفع علم بنما، بنقل الديزل البحري على التوالي إلى الناقلتين *Sam Jong 2* و *Rye Song Gang 1* اللتين ترفعان علم جمهورية كوريا الشعبية الديمقراطية، وذلك في ١٩ أكتوبر ٢٠١٧. وأبحرت الناقلتان من ميناء Yeosu، في جمهورية كوريا، وأقفلتا نظامهما الآلي لتحديد هويتهما بضعة أيام قبل عمليات النقل وبعدها. وأبحرت السفينتان جنوبا من أجل عمليات النقل، وليس إلى ميناء Taichung، مقاطعة تايوان الصينية، الذي كان ميناء

---

[26] تقرير فريق الخبراء بموجب قرار مجلس الأمن 1874، S/2017/150K، ص. 99
[27] تقرير فريق الخبراء المنشأ بموجب قرار مجلس الأمن 1874، S/2017/150K، ص. 101
[28] تقرير فريق الخبراء المنشأ بموجب قرار مجلس الأمن 1874، S/2019/691، ص. 9

المقصـــد المعلن، وعادتا بدلا من ذلك إلى ميناء Yeosu. واحتجزت جمهورية كوريا الناقلة *Lighthouse Winmore* لأغراض التحقيق في ٢٤ تشرين الثاني/نوفمبر ٢٠١٧[29].

عملية النقل من سفينة إلى سفينة بين سفينتَي Lighthouse Winmore و Sam Jong 2

المصدر: تقرير فريق الخبراء المنشأ بموجب قرار مجلس الأمن 1874، S/2018/171، ص. 33

استأجرت شركة Oceanic Enterprise Ltd من جزر مارشال الناقلة *Lighthouse Winmore* عن طريق وسيط مقره في سـنغافورة في الشـهر السـابق لعمليات النقل من سـفينة إلى سـفينة. ومدير هذه الشـركة ومسـاهمها الوحيد هو Shih-Hsien Chen (المعروف أيضـا باسـم "Sunny Chen")، وهو أحد مواطني مقاطعة تايوان الصـينية. كما أنّه المسـاهم والمالك والمشـغِّل الوحيد لسـفينتين وللشـركتين اللتين تملكهما، وهما الناقلة *Billions No. 18* وشـركة Bunker's Taiwan Group Corporation (جزر فرجن البريطانية)، وكذلك الناقلة *Billions No. 88* وشـركة Billions Bunker Group Corporation (جزر مارشـال)، التي شـاركت أيضـاً في عملية نقل إلى ناقلة أخرى لم تُحدَّد هويتها حتى الآن.

بالإضافة إلى ذلك، تَستخدِم ناقلتان من الناقلات العائدة لـ Chen، وهما *Lighthouse Winmore* و *Golden Rich*، نفس الجهة الحاملة لوثيقة الامتثال وجهة إدارة السلامة الدولية، وهي شركة Vanguard Shipping Safety Management Consultant Co. Ltd، التي تملك وتشغِّل الناقلة *Jin Hye* المشاركة في عمليات نقل من سفينة إلى أخرى[30].

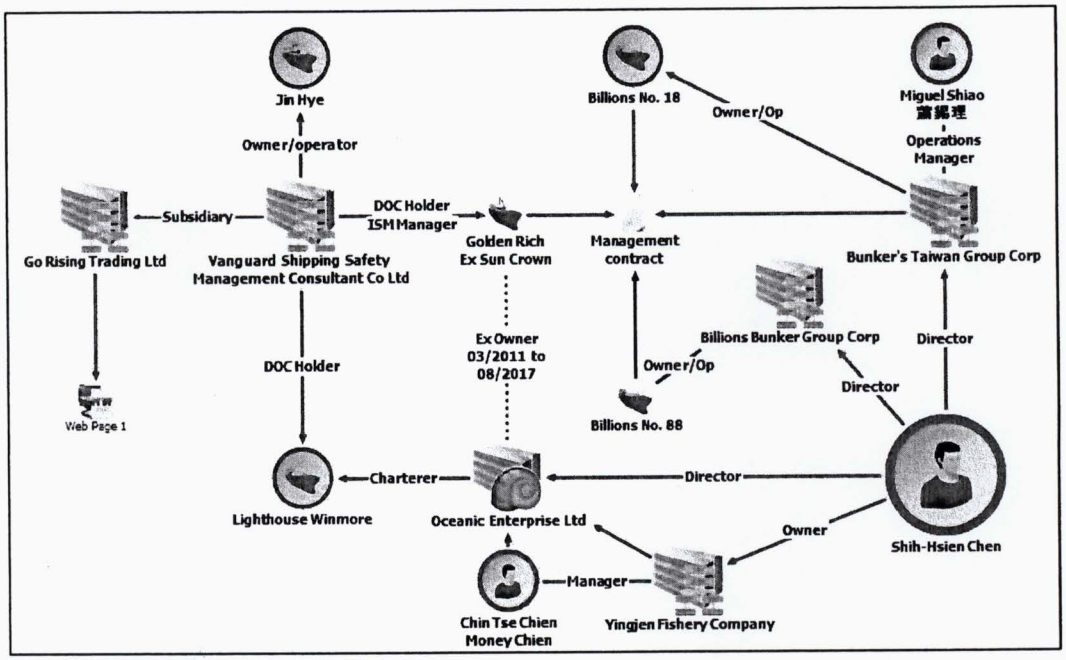
تُظهر بوليصـات الشـحن للمنتجات النفطية التي حمَلتها كل من الناقلتين *Lighthouse Winmore* (١٤ ٠٩٤ طنا متريا من زيت الغاز البحري (زيت الغاز)) و *Billions No. 18* (٧ ٩٥٤ طنا متريا من زيت الغاز (الديزل)) قبل عملية النقل في 19 أكتوبر ٢٠١٧ اسم الشركة المتعددة الجنسيات Trafigura Pte. Ltd، بوصفها الجهة الشاحنة، وشركة Global Commodities Consultants Ltd بوصفها الجهة المرسَل إليها، وميناء Taichung، بوصفه ميناء المقصد. وشركة Global Commodities مسجَّلة في هونغ كونغ، غير أن العنوان المسجَّل (12B Wilkinson Road, Singapore, 436759) يطابق عنوان الشـركة السـنغافورية Global SGP Pte Ltd (الرقم الفريد للكيان 201222231W)، وكلتا الشـركتين لهما نفس المدير والمسـاهم الوحيد. وعلاوة على ذلك، فإن جميع رسـائل البريد الإلكتروني المتعلقة بالشـحنات المحمَّلة على متن سـفن Chen وصـلت من شـركة Global SGP وليس من شـركة Global Commodities Consultants.

---

[29] تقرير فريق الخبراء المنشأ بموجب قرار مجلس الأمن 1874، S/2018/171، ص. 33

[30] تقرير فريق الخبراء المنشأ بموجب قرار مجلس الأمن 1874، S/2018/171، ص 37-38.

الناقلات الضالعة في عمليات النقل غير المشروعة والمرتبطة بـ Shih-Hsien Chen

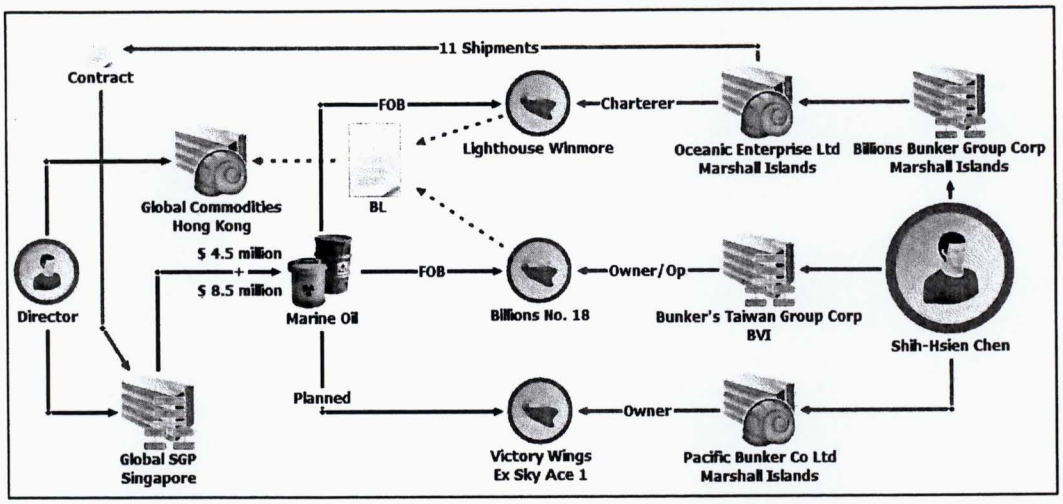


المصدر: تقرير فريق الخبراء المنشأ بموجب قرار مجلس الأمن 1874، S/2018/171، ص 38

وسددت شركة Oceanic Enterprise مقدما لشركة Global SGP أجور الشحنتين المسلَّمتين على متن السفينتين (4،564،942.80 دولار و8،510،097.75 دولار) عن طريق تحويلات مصرفية إلى الجهة المورِّدة التي كان لها عقد معها. وبالإضافة إلى عمليتي النقل هاتين اللتين قامت بهما الناقلتان *Billions No. 18* و*Lighthouse Winmore*، خططت شركة Oceanic للقيام بتسع شحنات أخرى باستخدام نفس السفينتين إضافة إلى سفينة أخرى من سفن Chen، هي *Sky Ace 1* وقد بلغ وزن تلك الشحنات وفقا للخطة الموضوعة لها ٠٠٠ ٩٥ طن متري (وتُقدَّر قيمتها بحوالي ٦٥ مليون دولار حسب السعر المستخدم في حساب الشحنتين الأُوليين المنقولتين إلى جمهورية كوريا الشعبية الديمقراطية)[31].

[31] تقرير فريق الخبراء المنشأ بموجب قرار مجلس الأمن 1874، S/2018/171، ص. 40

عمليات نقل النفط باستخدام الناقلات العائدة لـChen



المصدر: تقرير فريق الخبراء المنشأ بموجب قرار مجلس الأمن 1874، S/2018/171، ص 40

إساءة استخدام الكيانات الاعتبارية أو الترتيبات القانونية

تستخدم جمهورية كوريا الديمقراطية الشعبية المشاريع المشتركة والكيانات التعاونية وغيرها من الترتيبات القانونية للتهرّب من العقوبات أو مخالفتها. وكردّ على هذا الأمر، حظرت لجنة مجلس الأمن المنشأة بموجب القرار 1718 والقرارات المرتبطة بها تحت قرار مجلس الأمن 2375 (2017) في الفقرة 18، افتتاح وتعهّد وتشغيل جميع المشاريع المشتركة أو الكيانات التعاونية، الجديدة منها والقائمة، مع كيانات أو أفراد تابعين لجمهورية كوريا الشعبية الديمقراطية سواء كانوا يعملون لحساب حكومة جمهورية كوريا الشعبية الديمقراطية أو بالنيابة عنها أم لا.

مجموعة GENCO/KOGEN

لقد تم نشر هذه القضية في تقرير فريق الخبراء المنشأ بموجب القرار 1874 في مارس 2019 وأغسطس 2019، حول شركة Korea General Corporation for External Construction (المعروفة أيضاً بإسمي GENCO وKOGEN)، وهي شبكة من الكيانات الاعتبارية والترتيبات القانونية المسجّلة في دول مختلفة والمرتبطة بالمكتب العام للاستطلاع، وهي وكالة استخبارية كورية شمالية تدير العمليات السرية للدولة.

وأظهر التحقيق الذي يُجريه الفريق بشأن شركة GENCO/KOGEN أنها تتمتع بحضور كبير وشبكة واسعة النطاق في العديد من البلدان في الشرق الأوسط وأفريقيا والمنطقة الأوروبية الآسيوية، حيث تستخدم يداً عاملة وكيانات تعاونية ومشاريع مشتركة محظورة تابعة لجمهورية كوريا الشعبية الديمقراطية، وتحقق إيرادات كبيرة. ووفقاً لإحدى الدول الأعضاء، فإن شركة GENCO/KOGEN عملت على توفير اليد العاملة الكورية الشمالية في منطقة الشرق الأوسط بغرض جلب

العملة الصعبة لـــ [الحكومة] الكورية الشمالية". وتبيّن من تحقيقات الفريق أن ثمة أدلة على وجود نشاط لشركة KOGEN عن طريق مشروع مشترك مع شركة تابعة للإمارات العربية المتحدة[32].

ووفقاً لوثائق تسجيل المؤسسات التجارية، فإن شركة GENCO هي المالك الجزئي لكيان تعاوني أو لمشروع مشترك في مجال التشييد في الاتحاد الروسي، وهو "SAKORENMA" LLC، في حين أن نصيب الأغلبية من الملكية يعود إلى أحد الرعايا الروس. ويحتفظ هذا الكيان التعاوني أو المشروع المشترك بحساب في أحد المصارف الروسية. وعلاوة على ذلك، تتقاسم الشركة عناوينها ومعلومات الاتصال الخاصة بها وحَمَلة أسهمها مع ثلاث شركات أخرى منخرطة جميعها في أنشطة ذات صلة بالتشييد. كما تُظهِر وثائق تسجيل المؤسسات التجارية أن شركة GENCO تُشغِّل مكتبين تمثيليين رسميين في الاتحاد الروسي، أحدهما في فلاديفوستوك (Vladivostok) والآخر في خاسان (Khasan)، ويوظفان معاً 17 من الرعايا الأجانب رسمياً[33].

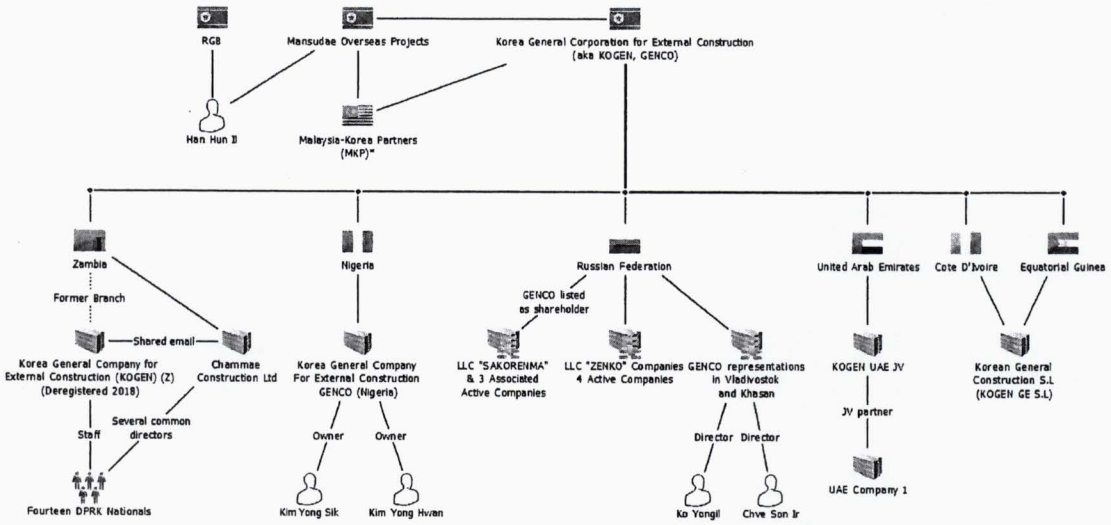
ويشمل وجود شركة GENCO/KOGEN في أفريقيا كلا من نيجيريا وكوت ديفوار وغينيا الاستوائية. فالشركة في نيجيريا مسجلة تحت اسم "Korea General Company for External Construction GENCO (Nigeria)". وفي كوت ديفوار، سُجلت شركة "Korea General Construction SL (KOGEN GE SL)" في عام 2012. ويذكر الموقع الشبكي لمكتب البلدان الأفريقية للموارد الحيوانية التابع للاتحاد الأفريقي شركة KOGEN GE S.L. بوصفها الجهة الشريكة له في تنفيذ مشروع تموله غينيا الاستوائية. وأُبلِغ عن شركة KOGEN بصورة منفصلة بوصفها جهة متعاقدة في مشروع ملعب ريبولا البلدي (Rebola Municipal Stadium) الذي أُنجِز في عام 2016 والذي تشير وثائقه إلى أن شركة KOGEN جنت منه حوالي 30.5 مليون دولار. وتقول الأنباء المحلية إن شركة KOGEN فتحت مقراً وطنياً جديداً كبير الحجم في غينيا الاستوائية في العام نفسه[34].

وأظهر تحليل الحسابات المصرفية لشركة GENCO/KOGEN في زامبيا، بالدولار وبالعملة المحلية، نشاطاً منتظماً، نقداً وبالشيكات، وحجماً كبيراً من التداول. وأظهرت الحسابات أنماطاً متماثلة في إيداع الشيكات، تليها تحويلات واردة، ومن ثم عمليات سحب منتظمة بالشيكات[35].

---

[32] تقرير فريق الخبراء المنشأ بموجب قرار مجلس الأمن 1874، S/2019/171، ص. 66
[33] تقرير فريق الخبراء المنشأ بموجب القرار 1874، S/2019/171، ص. 67
[34] تقرير فريق الخبراء المنشأ بموجب القرار 1874، S/2019/171، ص. 67
[35] تقرير فريق الخبراء المنشأ بموجب القرار 1874، S/2019/171، ص. 66

شبكة GENCO



المصدر: تقرير فريق الخبراء المنشأ بموجب القرار 1874، S/2019/171، ص. 68

مجموعة غلوكوم (Glocom)

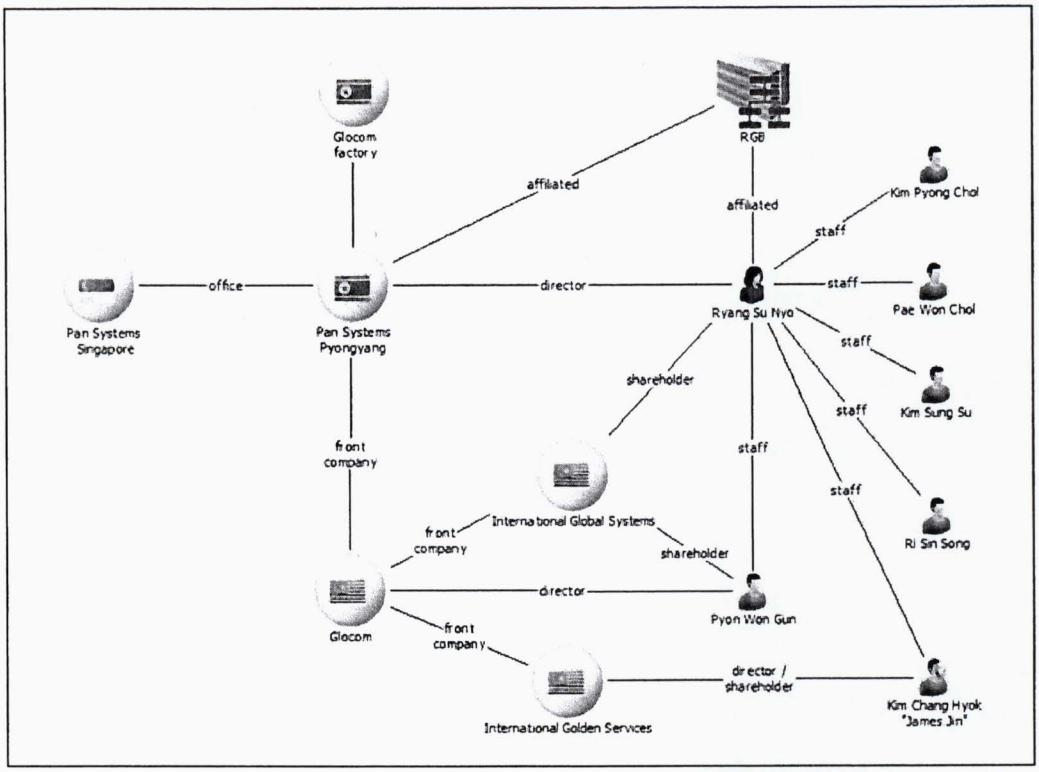
شركة Glocom هي شركة مقرها في ماليزيا وهي تُعلن عن معدات الاتصالات اللاسلكية للمنظمات العسكرية وشبه العسكرية. وتدَّعي شركة Glocom أنه لها وجود في أكثر من 10 بلدان وسمعة دولية بارزة اكتسبتها من خلال مشاركتها، حسب موقعها الشبكي، ثلاث مرات في معرض أسلحة "خدمات الدفاع في آسيا" منذ عام 2006 الذي يُعقد كل سنتين. وفي حين أن شركة Glocom غير مسجلة رسمياً وليس لها وجود في عنوانها المادي المدرج، هناك شركتان موجودتان في ماليزيا تتصرفان باسمها، وهما: International Golden Services Sdn Bhd و International Global Systems Sdn Bhd[36].

وتبيّن المعلومات التي حصل عليها الفريق أن شركة Glocom هي شركة صورية لشركة في جمهورية كوريا الشعبية الديمقراطية هي فرع بونغيانغ من شركة (Pan Systems Pyongyang)، وهي مرتبطة بشركة سنغافورية اسمها (Pan Systems Singapore)[37].

وفقا للمعلومات التي حصل عليها الفريق، فإن شركة Pan Systems Pyongyang يديرها المكتب العام للاستطلاع، وهو وكالة الاستخبارات الرئيسية في البلد، وهو مُدرج بموجب القرار 2270 (2016). وهذا يبيّن كيف يمكِّن المكتب عملاءه الرئيسيين من توليد الإيرادات لعملياته عن طريق هذه الشبكات. وبالإضافة إلى ذلك، قرر الفريق أن اسم شركة "Wonbang Trading Co." هو اسم آخر لشركة Pan Systems Pyongyang. وتبين المعلومات أيضاً أن شركة Pan Systems Pyongyang تتلقى بانتظام أموالاً من شركة Korea Mining Development Trading Corporation (KOMID)[38].

---

[36] تقرير فريق الخبراء المنشأ بموجب القرار 1874، S/2017/150، ص. 41
[37] تقرير فريق الخبراء المنشأ بموجب القرار 1874، S/2017/150، ص. 41
[38] تقرير فريق الخبراء المنشأ بموجب القرار 1874، S/2017/150، ص. 43



شبكة شركة Pan Systems Pyongyang

مصدر: تقرير فريق الخبراء المنشأ بموجب القرار 1874، S/2017/150، ص. 44

العمليات المالية لشركة Glocom/Pan Systems Pyongyang

واستفادت شركة Pan Systems Pyongyang وشركاتها الصورية في عملياتها المصرفية من شبكة واسعة من الأفراد والشركات والحسابات المصرفية الخارجية لشراء الأسلحة والأعتدة ذات الصلة وتسويقها. وتألفت الشبكة العالمية من أفراد وشركات وحسابات مصرفية في إندونيسيا وسنغافورة والصين وماليزيا والشرق الأوسط. وقد جرى تحديداً تحويل مبلغ 36،939 يورو إلى شركة International Global Systems في عام 2008 من حساب في فرع مصرف شرق أوسطي في دمشق[39].

منذ العام 1998، تستخدم شركتا Pan Systems Pyongyang و International Global System حسابات بالدولار الأميركي واليورو في مصرف Daedong Credit Bank (وهو مصرف تابع لجمهورية كوريا الديمقراطية الشعبية) للنفاذ إلى النظام المالي العالمي، بسبل منها حسابات مصرفية في الصين. واستخدمت هذه الحسابات لتحويل الأموال إلى سلسلة إمدادات لأكثر من 20 شركة تقع في بر الصين الرئيسي بشكل أساسي وفي هونغ كونغ، الصين وفي سنغافورة. وفي السنوات الأخيرة، تحولت عمليات الشراء بالكامل تقريباً إلى شركات في الصين وهونغ كونغ، الصين. ووفرت غالبية هذه الشركات منتجات إلكترونية ومكونات أجهزة الراديو وغلافاتها الخارجية بما يتماشى مع معدات الاتصالات العسكرية التي تسوق لها شركة Glocom، أما الشركات الأخرى فهي تعمل في مجال النقل. وأجرت الشبكة

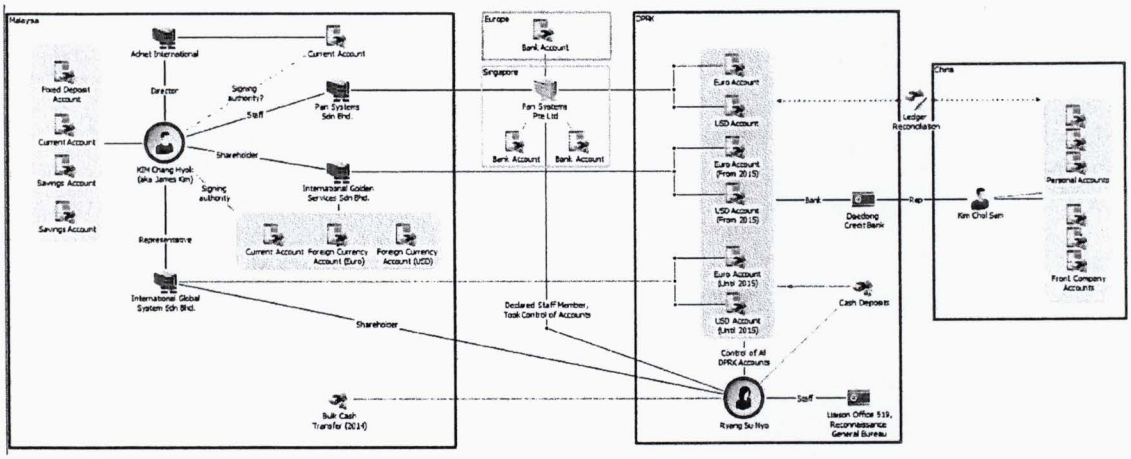
[39] تقرير فريق الخبراء المنشأ بموجب القرار 1874، S/2017/150، ص. 98

أيضاً تحويلات منتظمة إلى وسطاء مختلفين يحملون أسماء صينية وكورية وأجنبية وأسماء مشفرة، يعملون في إندونيسيا والصين وماليزيا والشرق الأوسط[40].

وفيما يتعلق بالتحويلات الواردة، تلقت شركة Pan Systems Pyongyang تحويلات ضخمة من حساب في مصرف كبير في ماليزيا، ومن شركات عديدة في جمهورية كوريا الشعبية الديمقراطية. كما تلقت شركة Pan Systems Pyongyang تحويلات نقدية ضخمة على نحو منتظم. وبالإضافة إلى ذلك، تلقت شركة Pan Systems Pyongyang أموالاً من كيانين مدرجين في القائمة، وهما شركتا KOMID و Hyoksin Trading Corporation. وبين عامَي 2011 و2013، أجرت شركة Hyoksin عدة تحويلات باليورو إلى شركة Pan Systems Pyongyang شأنها شأن شركة KOMID بين عامي 2011 و2015[41].

وسيطرت شبكة Glocom، إضافة إلى حساباتها المصرفية الأربعة لدى مصرف Daedong Credit Bank في بيونغ يانغ، على عشرة حسابات على الأقل في أربعة بلدان أخرى بين عامي 2012 و 2017، بما في ذلك من خلال شركات صورية مقيمة في ماليزيا. وتُبيّن السجلات أن هذه الحسابات المتعددة في الخارج سمحت لشركة Glocom، في سياق عملياتها التجارية غير المشروعة، بالنقل المستمر للأموال بين الحسابات التي تسيطر عليها في مصارف وبلدان مختلفة[42].

الحسابات التي تسيطر عليها شركة Glocom



المصدر: تقرير فريق الخبراء المنشأ بموجب القرار 1874، S/2018/171، ص. 76

[40] تقرير فريق الخبراء المنشأ بموجب القرار 1874، S/2017/150، ص. 98
[41] تقرير فريق الخبراء المنشأ بموجب القرار 1874، S/2017/150، ص. 99
[42] تقرير فريق الخبراء المنشأ بموجب القرار 1874، S/2018/171، ص. 75

المراجع

Financial Action Task Force, February 2015. *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL),* Paris: FATF.

Financial Action Task Force, October 2013. *The Role of Hawala and Oter Similar Service Providers in Money Laundering and Terrorist Financing,* Paris: FATF.

Financial Action Task Force, October 2015. *Emerging Terrorist Financing Risks,* Paris: FATF.

Panel of Experts pursuant to UNSCR 1874, S/2020/151. *Report of the Panel of Experts established pursuant to UNSCR 1874,* New York: United Nations Security Council.

Panel of Experts pursuant UNSCR 1874, S/2017/150. *Report of the Panel of Experts established pursuant to resolution 1874,* New York: United Nations Security Council.

Panel of Experts pursuant UNSCR 1874, S/2018/171. *Report of the Panel of Experts pursuant UNSCR 1874,* New York: United Nations Security Council.

Panel of Experts pursuant UNSCR 1874, S/2019/171. *Panel of Experts Report Pursuant UNSCR 1874 S/2019/171,* New York: United Nations Security Council.

Panel of Experts pursuant UNSCR 1874, S/2019/691. *Report of the Panel of Experts established pursuant to resolution 1874 (2009),* New York: United Nations Security Council.

United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015), S/2020/493. *The joint report of the Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015),* New York: United Nations Security Council.

United Nations Office on Drugs and Crime, 2012. *The Use of the Internet for Terrorist Purposes,* New York: UNODC.

www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware, 2018. *FASTCash: How the Lazarus Group is emptying millions from ATMs..* [Online] Available at: www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware.

United Nations Targeted Sanctions against the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction

Typologies paper

Content

Introduction

The United Nations Security Council (UNSC), pursuant to Chapter VII of the United Nations Charter with the aim to maintain peace and security, through its Resolutions and sanctions committees, mandates the implementation of 14 sanctions regimes which focus on supporting political settlement of conflicts, nuclear non-proliferation, and counter-terrorism.

This document is focused only on the following UNSC sanctions regimes:

- Terrorism and terrorist financing to:
  - Islamic State in Iraq and the Levant (Da'esh), Al-Qaida, and associated individuals, groups, undertakings and entities, and
  - The Taliban, and associated individuals, groups, undertakings, and entities.
- Proliferation of weapons of mass destruction and its financing to:
  - The nuclear-related, other weapons of mass destruction-related and ballistic missile-related programmes of the Democratic People's Republic of Korea (DPRK), and
  - The nuclear programme of the Islamic Republic of Iran (Iran).

This document presents cases and examples on how these sanctioned activities, persons, groups or entities have received financing and support, therefore in violation or evasion of UNSC Resolutions (UNSCR) related to:

All information presented in this document is derived from public sources. It includes a compilation of cases and situations, aiming to provide guidance to public and private institutions on trends and methods used by sanctioned persons, groups or entities to circumvent the UNSCR. It is the responsibility of each institution to implement adequate measures to prevent being misused to breach the UNSCR and duly report to the competent authorities any (attempted) circumvention.

Terrorist Financing

The term terrorist financing includes the provision of funds to commit terrorist activities and the support and maintenance of the person (terrorist) or the terrorist group. This includes providing food, lodging, training, making means available such us transportation, communication equipment. Such financing can take place with money or in kind, and funds involved can be from legal or illegal sources.

The following are methods and cases that illustrate how terrorist groups have misused economic sectors or activities to fund their activities. This document compiles information from documents developed by the UNSC, the United Nations Office on Drugs and Crime (UNODC) and the Financial Action Task Force (FATF).

Terrorist financing methods

In its report "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)" of 2015 FATF identified that this terrorist organization earns revenue primarily from five sources: (1) illicit proceeds from occupation of territory, such as bank looting, extortion, control of oil fields and refineries, and robbery of economic assets and illicit taxation of goods and cash that transit territory where ISIL operates; (2) kidnapping for ransom; (3) donations including by or through non-profit organisations; (4) material support such as support associated with FTFs and (5) fundraising through modern communication networks[1].

The Joint report of the Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) concerning Islamic State in Iraq and the Levant (ISIL) (Da'esh), Al-Qaida and the Taliban and associated individuals and entities on actions taken by Member States to disrupt terrorist financing, prepared pursuant to paragraph 37 of UNSCR 2462 (2019), of June 3 of 2020 ("Joint report") concludes from a questionnaire sent to all United Nations Member States that the most frequently used channels for terrorist financing are (1) the formal banking system; (2) cash smuggling; (3) the money services business; and (4) informal remitters or hawala[2].

The Joint report also reports on the abuse of technology (including social media, prepaid cards and mobile banking) for terrorist purposes, noting that terrorist financing was facilitated by recent developments in mobile payments and the anonymity of money transfers and illicit donations via crowdfunding platforms.[3]

The UNSC notes that terrorists and terrorist groups raise funds through a variety of means, including exploitation of natural resources, kidnapping for ransom and links to organized crime and drug trafficking. The Joint report notes the potential for terrorism financing through the construction and real estate sectors, the use of shell companies to conceal cash, the use of non-profit organizations and trade-based terrorism financing.[4]

---

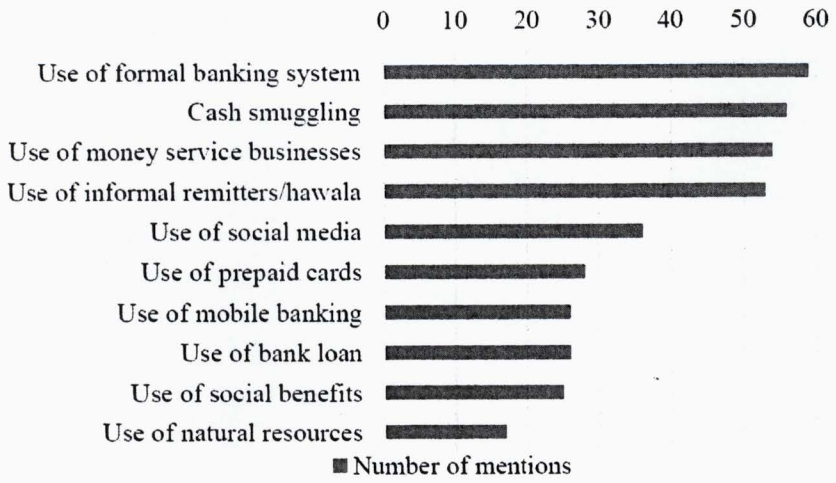
[1] Financial Action Task Force, 2015, p. 12

[2] United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) , S/2020/493, p. 16.

[3] United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) , S/2020/493, p. 17.

[4] United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) , S/2020/493, p. 17.

Methods most frequently used by terrorist financiers



Source: United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015), S/2020/493, p. 16.

Banking services

The formal banking system is vulnerable for terrorist financing because of the difficulty of distinguishing between legitimate and illegitimate low-cost transactions and detecting indirect transactions. Transaction-monitoring programmes are often unable to identify terrorism financing. There is also a risk in the use of bank loans and social benefits payed through banks for terrorist financing.[5]

Continued Access to bank accounts by Foreign Terrorist Fighters

According to sensitive financial information, terrorist financing risks were discovered regarding foreign cash withdrawals via ATMs that were made in areas located near territories where ISIL operates by unknown individuals. These withdrawals were taken from US-based bank accounts using a check card. Another terrorist financing risk identified was the existence of large deposits into bank accounts followed by immediate foreign cash withdrawals in areas located near to territories where ISIL operates. This information reveals the terrorism financing risks posed by the continued ability of the individuals who are believed to have travelled to areas occupied by ISIL to reach their bank accounts in their home countries. *Source: United States*.[6]

Money remitters

Along with the banking sector, the remittance sector has been exploited to move illicit funds and is also vulnerable to Terrorist Financing. In countries where access to banking services is limited, remittance providers may be the primary financial institution through which consumers can engage in cross-border funds transfer activity. Remittance providers are especially vulnerable to abuse for

[5] United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) , S/2020/493, p. 16.
[6] Financial Action Task Force, February 2015, p. 23

Terrorist Financing where they are unregulated, not subject to appropriate AML/CFT supervision or where they operate without a license (thus operating without any AML/CFT controls)[7].

Complicit MVTS Agent

An individual raised funds for Al-Shabaab from within the Somali diaspora in Missouri and elsewhere and used a variety of licensed money service businesses (MSBs) with offices in the United States to remit the money to Somalia for general support of Al-Shabaab fighters. The co-conspirator, who worked for one of the MSBs involved, helped the individual avoid leaving a paper trail by structuring transactions into low dollar amounts and by using false identification information. The MSB worker and other conspirators used fictitious names and phone numbers to hide the nature of their transactions[8].

Hawala and Other Similar Service Providers (HOSSP)

There are several reasons why HOSSPs poses a terrorist financing vulnerability, including: a lack of registration and supervision, settlement across multiple jurisdictions through value or cash outside of the banking system in some cases, the use of businesses that are not regulated financial institutions, the use of net settlement and the commingling of licit and illicit proceeds[9].

Terrorist Abuse of HOSSPs

A sum of INR 10 000 000 (USD 160 000) was intercepted in a State A in India which was meant to be delivered to a terrorist gang X. Investigation revealed that a number of earlier consignments had earlier been delivered to the terrorist gang earlier. It was revealed that development funds of a particular area in that State was defalcated and then sent to location P in that State. From location P, it was sent to location Q in another State B with the help of hundi operators operating between State A and State B. The hundi operators are told that the money belongs to a very influential person at state A. The hundi operators do not object conducting the transaction hearing the name of this influential person and deliver the money at state B to the person authorized by the agent of the terrorist gang. The money is delivered after deducting a commission of 1 per cent from the total money which is transferred. At State B, the hawala money is then changed from INR to Dollars in an unregulated exchange market and then transferred to another country E where arms and ammunition are purchased by the terrorist gang leaders based there. These arms and ammunition are then transferred across the borders and then delivered to the terrorist gang operating in State A for carrying our terrorist activities. In this case a total of 15 accused were arrested and charge sheeted, and the trial is being held. The arrested members include terrorists, contractors, agents, and government servants[10].

Online payment facilities

Online payment facilities offered through dedicated websites or communications platforms make it easy to transfer funds electronically between parties. Funds transfers are often made by electronic

[7] Financial Action Task Force, October 2015, p.26
[8] Financial Action Task Force, October 2015, p. 26
[9] Financial Action Task Force, October 2013, p. 41
[10] Financial Action Task Force, October 2013, p. 43

wire transfer, credit card or alternate payment facilities available via services such as PayPal or Skype.[11]

Fundraising through the Internet

Intelligence information indicates that some individuals associated with ISIL have called for donations via Twitter and have asked the donors to contact them through Skype. The donors would be asked to buy an international prepaid card (e.g., a credit for a mobile line or to purchase an application or other program which stores credit) and send the number of the prepaid card via Skype. The fundraiser would then send the number to one of his followers in close country from Syria and sell the number of the card with a lower price and take the cash which was afterwards provided to ISIL. Source: Saudi Arabia[12].

PayPal accounts used for fundraising

A charity set up in 2010, whose chairman is specialised in e-marketing, offers on its website several options to make donations by credit card, PayPal, cash transfers, checks. Over a year and a half, bank accounts of this charity received numerous donations by checks and wire transfers below EUR 500. Of the EUR 2 million collected, EUR 600 000 came from a few PayPal transactions from another country. Personal PayPal accounts were also used to collects funds, then to be withdrawn by cash, or transferred to other accounts. Source: France[13].

Theft through online payment facilities

Online payment facilities can be vulnerable for identity theft, credit card theft, wire fraud, stock fraud, intellectual property crimes and auction fraud.

The United Kingdom case against Younis Tsouli: Profits from stolen credit cards were laundered by several means, including transfer through e-gold online payment accounts, which were used to route the funds through several countries before they reached their intended destination. The laundered money was used both to fund the registration by Tsouli of 180 websites hosting Al-Qaida propaganda videos and to provide equipment for terrorist activities in several countries. Approximately 1,400 credit cards were used to generate approximately £1.6 million of illicit funds to finance terrorist activity[14].

Donations including by or through non-profit organisations (NPOs)

Individuals and organisations seeking to fundraise for terrorism and extremism support may attempt to disguise their activities by claiming to be engaged in legitimate charitable or humanitarian activities and may establish NPOs for these purposes[15].

---

[11] United Nations Office on Drugs and Crime, 2012, p. 7
[12] Financial Action Task Force, February 2015, pp. 24-25
[13] Financial Action Task Force, October 2015, p. 38
[14] United Nations Office on Drugs and Crime, 2012, p. 7
[15] Financial Action Task Force, October 2015, p. 32

Diversion of Funds by Actors to NPOs

An individual (Mr. A) established a charitable foundation under the pretext of collecting donations for Syrian refugees, people in need of medical and financial aid, and construction of mosques, schools and kindergartens. However, Mr. A was the leader of an organized scheme in which donations were sent to a group of individuals related to Mr. A (Group A) instead of the foundation's account. In most cases, the first stage involved money being sent through money remitters and then transported in cash. The money was then transferred either to credit cards accounts or to e-wallets. The members of Group A placed the relevant information (that funds are being collected for the declared purposes) on the Internet, but, in fact, the funds were sent as an aid for terrorists and their families and meant to be used as a financial support for terrorist activities. This information was discovered through investigations conducted by the FIU based on regular monitoring of entities on their domestic list of designated terrorist entities and related persons or on information provided by law enforcement. Analysis of the collected information allowed the FIU to identify the relation between different cases: common payers and recipients and similar modus operandi in collection and distribution of funds. Further cooperation with law enforcement authorities allowed the FIU to establish the direct link between Mr. A and ISIL's activity. This resulted in several criminal investigations related to Mr. A. In addition, Mr. A was listed on the domestic list of designated terrorist entities, with the relevant freezing procedures performed. Under the court decisions, assets of the Group A members were frozen[16].

Cash Smuggling

Cash continues to be a prevalent aspect of terrorist operations. While funds may be raised in several ways, often they are converted into cash to be taken to conflict zones. This is assisted by porous national borders, difficulty in detecting cash smuggling (particularly in the small amounts that are sometimes smuggled for TF purposes), and the existence of informal and unregulated economies[17].

Cash couriers

Over a period of three consecutive days three individuals declared a total amount of some EUR 90 000 in cash to customs officials at the airport in Brussels. The funds are said to originate from NPO A from Germany as part of humanitarian aid in Burundi, Benin and Zimbabwe. The three couriers are all Belgian nationals and have been living in Belgium for a long time. Accounts were held by the three individuals. A Belgian coordinating body of a radical Islamic organisation transferred money to these accounts. Over a period of one year a total amount of nearly EUR 20 000 was withdrawn in cash. Some EUR 10 000 was transferred to Turkey.

According to the German FIU, NPO A was one of the largest Islamic organisations in Germany. NPO A is said to be linked with NPO B, which had been banned in Germany for allegedly supporting a terrorist organisation. All of NPO B's board members also played a major role in NPO A.

According to information from the Belgian intelligence services the three individuals reverenced above are known to be involved in local branches of a radical Islamic organisation. Given the nature of the transactions and the links between the two NPO referenced above, Belgian authorities suspect that at least part of the funds described above could have been used to support terrorist activities.[18]

---

[16] Financial Action Task Force, February 2015, p. 20
[17] Financial Action Task Force, October 2015, p. 23
[18] Financial Action Task Force, October 2015, p. 23

Financing the Proliferation of Weapons of Mass Destruction

The term proliferation of weapon of mass destruction (proliferation) does not limit itself to providing or allowing chemical, biological, radiological or nuclear material or equipment to build weapons but it also involves the transfer and export of technology, goods, software, services or expertise that could be used in nuclear, chemical or biological weapon-related programmes.

Therefore, Proliferation financing is providing financial services to those related programmes for the transfer and export of nuclear, chemical or biological weapons, their means of delivery and related materials. It also involves the financing of trade in sensitive goods needed to support or maintain those programmes, even if those goods are not related to any nuclear, chemical or biological material, for example: oil, coal, steel, military communication equipment. Additionally, proliferation financing includes the financial support to individuals or entities engaged in proliferation, even if they perform other activities that are nor related to such programmes, for example: diplomats, shipping companies, fisheries, trade in commodities companies.

The following are cases of violations or evasion of the sanctions imposed by the UNSC related to the Nuclear Programme of the Democratic People's Republic of Korea (DPRK), as presented by the Panel of Experts pursuant to UNSCR 1874, between 2017 and 2020 ("the Panel").

The cases that are explained here involve many sectors worldwide, including the financial, trade and shipping sectors, and evidence the need for countries to increase the awareness in all economic sectors about these sanctions and the importance of their implementation.

With regards to Iran, UNSCR 2231 of July 20, 2015 endorsed the Joint Comprehensive Plan of Action negotiated between Iran and the P5+1 (the five permanent members of the United Nations Security Council—China, France, Russia, United Kingdom, United States—plus Germany) which significantly reduced the sanctions regime related to Iran's nuclear programme. The verification process is currently more focused on the nuclear activity itself and carried out by the International Atomic Energy Agency (IAEA), thus not relevant for this document.

Financial measures

Financial assets

Financial activities of diplomatic and other personnel of the DPRK

The Panel investigated diplomatic or official personnel of the DPRK who act on behalf of the country's sanctioned financial institutions to establish illicit banking networks and provide the country with access to global banking systems.

The Panel investigated reports that Jo Kwang Chol, an accredited member of the administrative and technical staff at the Embassy of the DPRK in Austria since 2016, had engaged in sanctions evasion activities on behalf of the designated Foreign Trade Bank. According to information provided by Austria, Mr. Jo had attempted to gain access to Korea Ungum Corporation's frozen accounts at an Austrian bank. Austrian authorities froze the accounts in July 2015 owing to suspected money-laundering activity. At the time, the total balance was approximately $1,895,633[19].

[19] Report of the Panel of Experts pursuant to UNSCR 1874, S/2020/151, p. 63

Cyberactivity targeting financial institutions

There is evidence that DPRK by the means of cyberattacks is stealing funds from financial institutions and cryptocurrency exchanges in different countries, which allows the country to evade financial sanctions and generate income in ways that are harder to trace and subject to less government oversight and regulation. During 2019, there were investigations of at least 35 reported instances of DPRK actors attacking financial institutions, cryptocurrency exchanges and mining activity designed to earn foreign currency, including in the following Member States: Bangladesh (2 cases), Chile (2), Costa Rica (1), the Gambia (1), Guatemala (1), India (3), Kuwait (1), Liberia (1), Malaysia (1), Malta (1), Nigeria (1), Poland (1), the Republic of Korea (10), Slovenia (1), South Africa (1), Tunisia (1) and Viet Nam (1)[20].

According to the UN Panel of Expert pursuant resolution 1874 report S/2019/691, since 2019 there is a marked increase in the scope and sophistication of such cyberactivities. Some estimates placed the amount illegally acquired by the DPRK at as much as $2 billion[21].

Operation "FASTCash"

The Panel, in its report of August 2019, reported on a cyberattack carried out by DPRK cyber actors who gained access to the infrastructure managing entire automatic teller machine networks of a country. The purposes were to install malware modifying transaction processing in order to force 10,000 cash distributions to individuals working for or on behalf of the DPRK across more than 20 countries in five hours. That operation required large numbers of people on the ground, which suggests extensive coordination with DPRK nationals working abroad and possibly cooperation with organized crime[22].

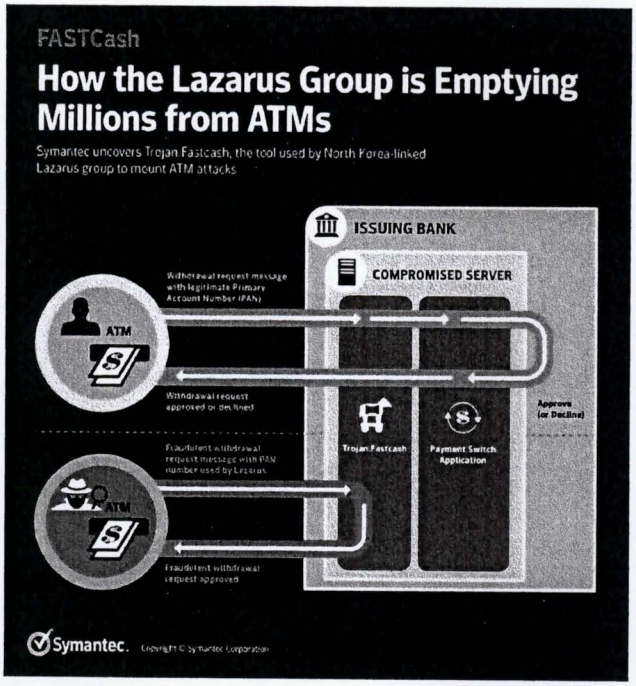
The operation, known as "FASTCash", was enabled by Lazarus, a group involved in both cybercrime and espionage, with apparent links to DPRK. With this operation it was possible to fraudulently empty ATMs of cash. To make the fraudulent withdrawals, Lazarus first breaches targeted banks' networks and compromises the switch application servers handling ATM transactions.

Once these servers are compromised, previously unknown malware (Trojan.Fastcash) was deployed. This malware in turn intercepts fraudulent Lazarus cash withdrawal requests and sends fake approval responses, allowing the attackers to steal cash from ATMs.

According to a U.S. government alert, one incident in 2017 saw cash withdrawn simultaneously from ATMs in over 30 different countries. In another major incident in 2018, cash was taken from ATMs in 23 separate countries. To date, the Lazarus FASTCash operation is estimated to have stolen tens of millions of dollars[23].

---

[20] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 26
[21] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 26
[22] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 26
[23] FASTCash: How the Lazarus Group is emptying millions from ATMs, Symantec, 2 October 2018. Available at www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware.



Source: "FASTCash: How the Lazarus Group is emptying millions from ATMs", Symantec, 2 October 2018. Available at www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware.

Cyberattack to cryptocurrency exchange bureaus

In 2019, DPRK cyber actors shifted focus to targeting cryptocurrency exchanges. Some cryptocurrency exchanges have been attacked multiple times, in particular those registered in the Republic of Korea. Bithumb was reportedly attacked by DPRK cyber actors at least four times. The first two attacks, in February and July 2017, resulted in losses of approximately $7 million each, with subsequent attacks in June 2018 and March 2019 resulting in the loss of $31 million and $20 million, respectively, showing the increased capacity and determination of DPRK cyber actors. Similarly, Youbit (formerly Yapizon) suffered multiple attacks involving a $4.8 million loss in April 2017 and then 17 per cent of its overall assets in December 2017, forcing the exchange to close[24].

Designated banks maintain representative offices and agents abroad

The Panel reported in February 2017 that it had obtained information showing that two UNSC sanctioned banks, Daedong Credit Bank (DCB) and Korea Daesong Bank (KDB), are both operating on Chinese territory, through representative offices in Dalian, Dandong and Shenyang. A director of such offices also served as a director of a designated company, DCB Finance Ltd., registered in the British Virgin Islands. DCB Finance shared several officers with DCB. When the DCB correspondent accounts were closed in 2005, DCB Finance was set up to undertake wire transfers and business transactions on its behalf[25].

The representative in Dalian of DCB and DCB Finance, undertook transactions worth millions of United States dollars, including several of $1 million or more. He also facilitated payments and loans between companies linked to DCB and exchanged large quantities of bulk cash transferred to China from the DPRK into newer and larger denomination United States dollar notes. He also regularly undertook

[24] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 28
[25] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 75

foreign exchange between United States dollars and euros and transferred balances between DCB and its shareholder, Korea Daesong Bank. When DCB established representative offices in Shenyang in late 2012, and Dandong in 2014, the three offices cooperated in managing the activities of foreign exchange, transfer, bulk cash exchange and loans[26].

Economic resources

Bulk cash and gold

Bulk cash and gold are used by the DPRK to transfer value by circumventing the formal financial sector entirely. The following are some cases reported by the Panel.

On 6 March 2015, Bangladesh seized 26.7 kg of gold bars and jewellery (worth $1.4 million) from the hand luggage of the First Secretary of the embassy of the DPRK in Dhaka. An invoice related to those goods had been issued by AMM Middle East General Trading in Dubai, United Arab Emirates, and they were collected from Singapore. The First Secretary had flown into and out of Singapore from Dhaka on the same day, leaving the airport for three hours. He had undertaken on average one such trip per month to Singapore over the previous 15 months from both Dhaka and Beijing (ranging from a few hours to two days on the ground), suggesting that he was serving as a regular diplomatic courier smuggling gold and other items in evasion of sanctions. He was accompanied by other diplomats of the DPRK on some of the trips[27] .

On 17 March 2016 in Sri Lanka, an overseas worker of the DPRK was arrested at the airport in Colombo carrying $167,000 in cash, gold jewellery and watches. He was en route from Oman to Beijing and made no customs declaration. He was accompanied by five other individuals from the DPRK who were working in Oman for a construction company of the DPRK based in Dubai with a post office box address. He produced a list with 311 names of workers of the DPRK whose families in Pyongyang he was to pay (with amounts varying from $200 to $1,500, with an average of around $300 per family)[28].

Oil ship-to-ship transfers

Since 2018, the Panel has evidence of an increasing frequency of ship-to-ship transfers and of one unprecedented prohibited petroleum product transfer comprising 57,623.491 barrels alone, worth $5,730,886. The Panel's investigation of this transfer reveals a very sophisticated case of DPRK-related vessel identity fraud, highlighting new sanction evasion techniques that defeated the due diligence efforts of the region's leading commodity trader, as well as the United States and Singaporean banks that facilitated the fuel payments and a leading United Kingdom insurer that provided protection and indemnity cover to one of the vessels involved. The case also underlines, once again, the extremely poor reporting, oversight, monitoring and control over the vessels exercised by the flag-of-convenience States under whose jurisdiction they apparently sail[29] and also the lack of implementation of freezing sanctions.

Lighthouse Winmore

In 2018 the Panel investigated four ships involved in the violation of paragraphs 11 and 14 of UNSCR 2375 (2017). Their activities were primarily based in Taiwan Province of China, their companies have

[26] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 76
[27] Report of the Panel of Experts pursuant to UNSCR 1874, S/2017/150, p. 79
[28] Report of the Panel of Experts pursuant to UNSCR 1874, S/2017/150, p. 79
[29] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 8

been registered in multiple jurisdictions, including the British Virgin Islands, Hong Kong, the Marshall Islands, Samoa and Seychelles, with ships flagged in Dominica, Hong Kong, Panama and Sierra Leone.

The first two tankers that the Panel investigated, the Hong Kong-flagged Lighthouse Winmore and the Panama-flagged Billions No. 18, transferred marine diesel to the DPRK-flagged tankers, the Sam Jong 2 and the Rye Song Gang 1, respectively, on 19 October 2017. Both tankers sailed from Yeosu, Republic of Korea, and switched off their Automatic Identification System a few days before and after the transfers. Both vessels sailed southwards for transfers, but not to the port of Taichung, Taiwan Province of China, the stated port of destination, instead returning to Yeosu. The Republic of Korea detained the Lighthouse Winmore for investigation on 24 November 2017[30].

Ship-to-ship transfer between the Lighthouse Winmore and the Sam Jong 2

Source: Report of the Panel of Experts pursuant UNSCR 1874 - S/2018/171 p. 29

The Lighthouse Winmore was chartered the month before the ship-to-ship transfers by the Marshall Islands company Oceanic Enterprise Ltd via a Singapore-based broker. Its sole director and shareholder is Shih-Hsien Chen (also known as "Sunny Chen"), a national of Taiwan Province of China.

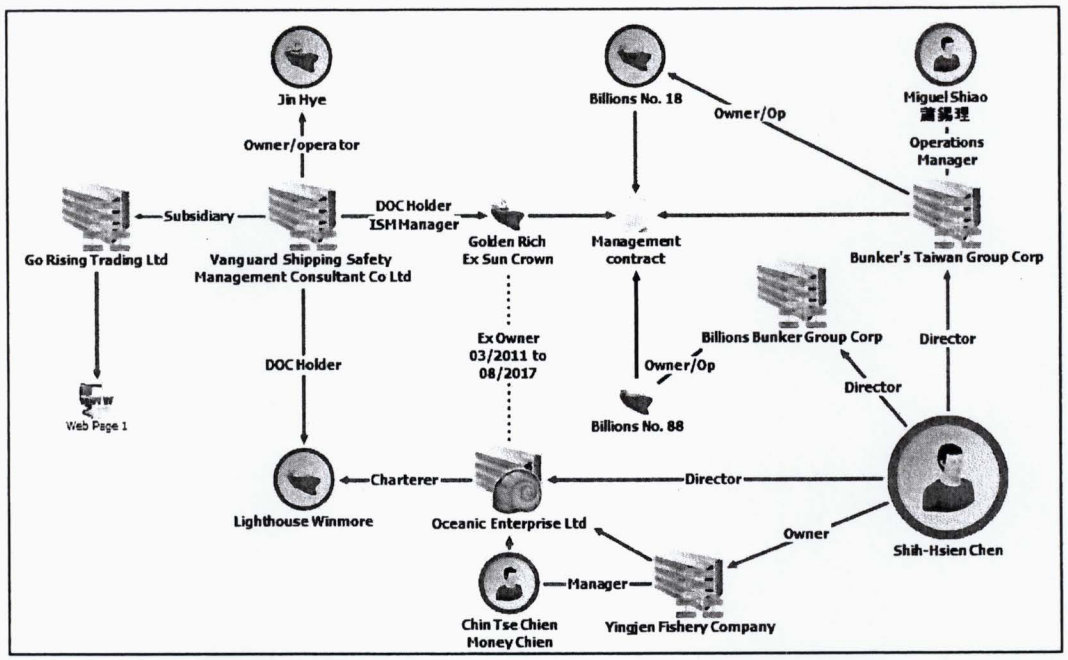
He is also the sole shareholder, owner and operator of two ships and the companies that own them, the tanker Billions No. 18 and Bunker's Taiwan Group Corporation (British Virgin Islands), as well as the tanker Billions No. 88 and the Billions Bunker Group Corporation (Marshall Islands), which has also engaged in ship-to-ship transfer to an as yet unidentified tanker.

In addition, two of Chen's tankers, the Lighthouse Winmore and the Golden Rich, utilize the same document of compliance holder and International Safety Management manager, Vanguard Shipping Safety Management Consultant Co. Ltd, which is the owner and operator of the other tanker engaging in ship-to-ship transfers, the Jin Hye[31].

The bills of lading for the petroleum products embarked by both the Lighthouse Winmore (14, 094 metric tons of marine gasoil (gasoil)) and the Billions No. 18 (7,954 metric tons of gasoil (diesel)) prior to the transfer on 19 October 2017 show the multinational company, Trafigura Pte. Ltd, as the shipper, Global Commodities Consultants Ltd. as the consignee and the port of Taichung as the destination. Global Commodities is registered in Hong Kong, but the registered address (12B Wilkinson Road, Singapore, 436759) matches that of the Singaporean company, Global SGP Pte Ltd. (Unique Entity No. 201222231W), both of which share the same director and sole shareholder. Further, all email communications for shipments onboard Chen's vessels came from Global SGP and not Global Commodities Consultants.

[30] Report of the Panel of Experts pursuant UNSCR 1874, S/2018/171, p. 29
[31] Report of the Panel of Experts pursuant UNSCR 1874, S/2018/171, pp. 32-33

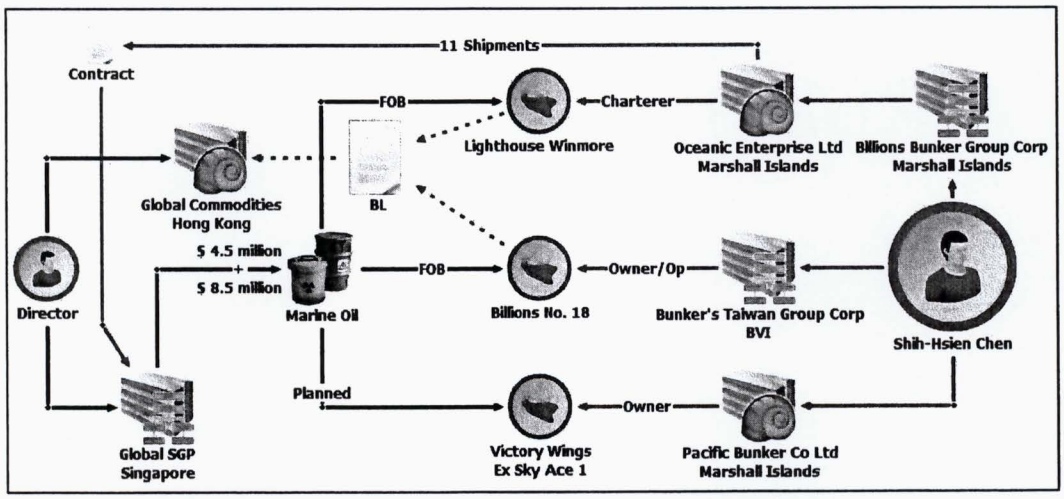
Tankers engaged in illicit transfers linked to Shih-Hsien Chen



Source: Report of the Panel of Experts pursuant UNSCR 1874 - S/2018/171 p.33

Oceanic Enterprise prepaid Global SGP Pte Ltd. for the two shipments delivered free onboard (FOB) to the vessels ($4,564,942.80 and $8,510,097.75) through bank transfers to the supplier, with which it had a contract. In addition to these two transfers by the Billions No. 18 and the Lighthouse Winmore, Oceanic had planned another nine shipments with the same two vessels plus another of Chen's vessels, the Sky Ace 1, which according to the plan for the shipments totalled 95,000 metric tons (with an estimated value of about $65 million according to the rate used for the first two transfers to the DPRK)[32].

Oil transfers using the tankers of Shih-Hsien Chen



Source: Report of the Panel of Experts pursuant UNSCR 1874 - S/2018/171 p.35

[32] Report of the Panel of Experts pursuant UNSCR 1874, S/2018/171, p. 34

Misuse of legal entities or arrangements

DPRK uses Joint ventures, cooperatives and other legal arrangements to evade or violate sanctions. As a response, the UNSC Committee pursuant to UNSCR 1718 and its related Resolutions prohibited under UNSC Resolution 2375 (2017), paragraph 18, the opening, maintenance and operation of joint ventures or cooperative entities, new or existing, with DPRK entities or individuals, whether or not acting for or on behalf of the government of the DPRK.

The GENCO/KOGEN Group

This is a case, published in the Panel of Experts report pursuant to resolution UNSCR 1874 in March 2019 and August 2019, involving the Korea General Corporation for External Construction (a.k.a. GENCO, a.k.a. KOGEN) group, a network of legal companies and arrangements registered in different countries linked with the Reconnaissance General Bureau, a North Korean intelligence agency that manages the state's clandestine operations.

The Panel of Experts reported on the ongoing investigation into GENCO/KOGEN that showed that the company has a large reach and extensive network in several countries in the Middle East, Africa and Eurasia, where it utilizes labourers, prohibited cooperative entities and joint ventures of the DPRK and earns significant revenue. According to a country, GENCO/KOGEN "has worked to supply North Korean laborers in the Middle East for the purpose of earning hard currency for [the] North Korea[n government]".The Panel's investigations found evidence of KOGEN activity by a joint venture with a company of the United Arab Emirates[33].

According to corporate registration documents, GENCO is the partial owner of a construction cooperative entity or joint venture company in the Russian Federation, LLC "SAKORENMA", with majority ownership belonging to a Russian national. This cooperative entity or joint venture maintains an account with a Russian bank. Furthermore, the company shares addresses, contact information and shareholders with three other companies, all of which engage in construction-related activities. In addition, corporate registry documents show that GENCO operates two official representative offices in the Russian Federation, one in Vladivostok and one in Khasan, that together formally employ 17 foreign nationals.[34]

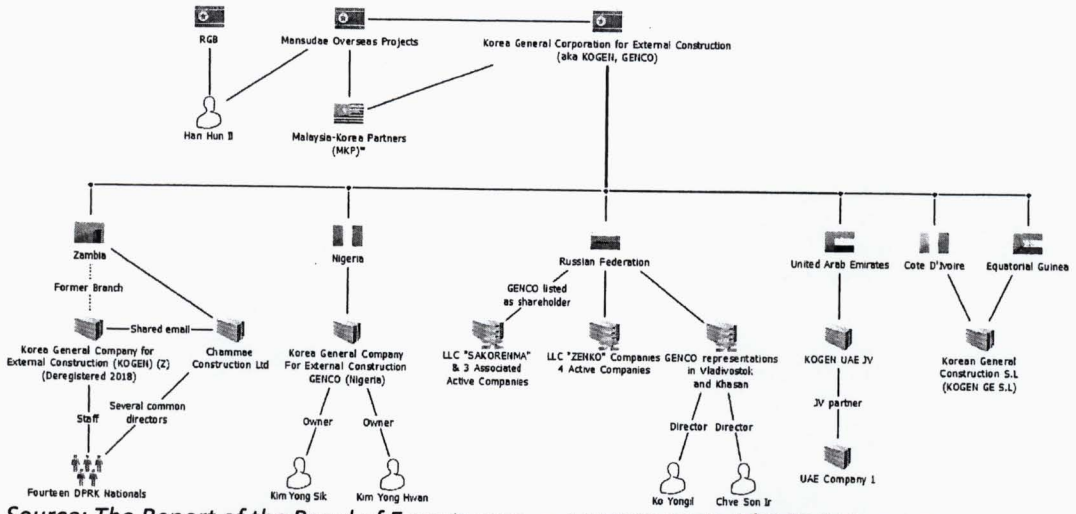
The presence of GENCO/KOGEN in Africa covers Nigeria, Côte d'Ivoire and Equatorial Guinea. In Nigeria, it is registered as "Korea General Company for External Construction GENCO (Nigeria)." In Côte d'Ivoire, "Korea General Construction SL (KOGEN GE SL)" was registered in 2012.The website of the African Union Inter-African Bureau for Animal Resources lists KOGEN GE S.L. as its implementing partner for a project funded by Equatorial Guinea. KOGEN was separately reported as a contractor for the Rebola Municipal Stadium, completed in 2016, which documents suggest earned KOGEN approximately $30.5 million. Local news claims that KOGEN opened a new, large national headquarters in Equatorial Guinea the same year[35].

Analysis of GENCO/KOGEN bank accounts in Zambia, in dollars and in local currency, showed regular cash and cheque activity and high account turnover. The accounts demonstrated similar patterns of cheque deposits, followed by incoming transfers, followed by regular cheque withdrawals[36].

---

[33] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/171, p. 56
[34] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/171, p. 56
[35] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/171, p. 56
[36] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/171, p. 55

GENCO network



Source: The Report of the Panel of Experts pursuant UNSCR 1874, S/2019/171, p. 57.

The Glocom group

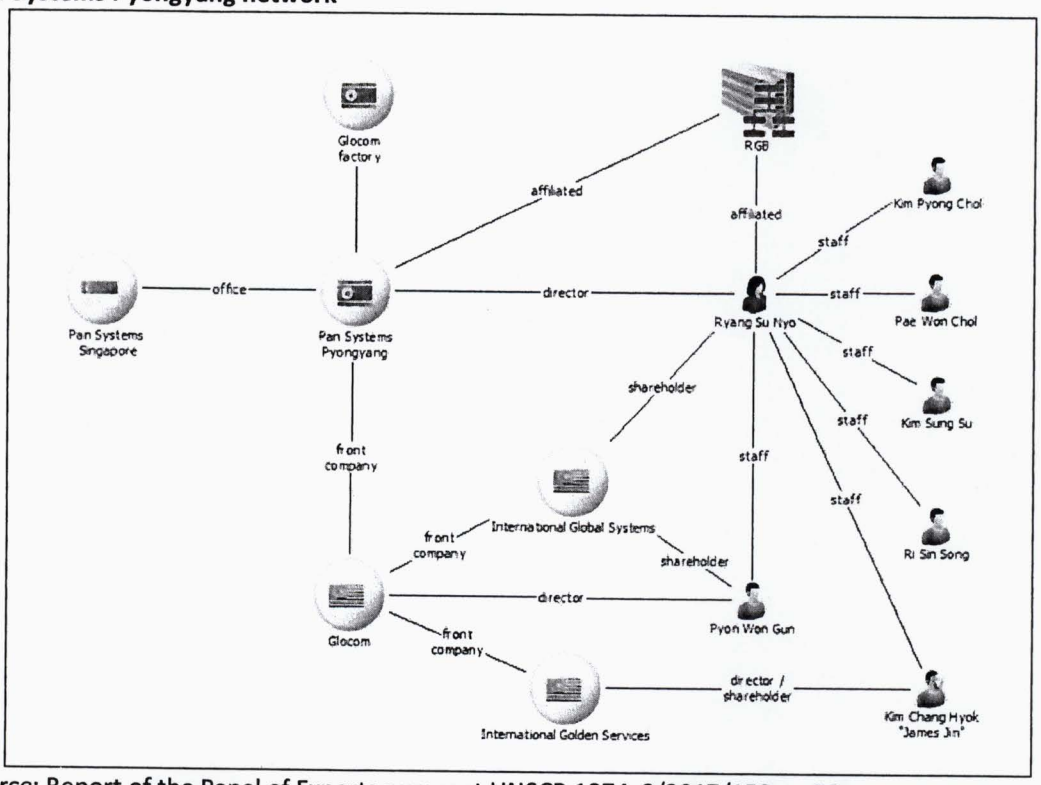
Glocom is a Malaysia based company which advertises radio communications equipment for military and paramilitary organizations. Glocom claims a presence in more than 10 countries and a prominent international reputation gained through participating, according to its website, in three biennial "Defense Service Asia" arms exhibitions since 2006. However, Glocom is not officially registered and has no presence at its listed physical address. Two other Malaysia based companies acted on its behalf: International Golden Services Sdn Bhd and International Global Systems Sdn Bhd[37].

Information obtained by the Panel demonstrates that Glocom is a front company of the DPRK company Pan Systems Pyongyang Branch (Pan Systems Pyongyang), which is linked to a Singaporean company named Pan Systems (S) Pte Ltd (Pan Systems Singapore)[38].

According to information obtained by the Panel, Pan Systems Pyongyang is operated by the Reconnaissance General Bureau, the country's premier intelligence agency, designated under UNSCR 2270 (2016). This shows how the Bureau enables its key agents to generate revenues for its operations through such networks. Additionally, the Panel determined that "Wonbang Trading Co." is an alias of Pan Systems Pyongyang. Information shows that Pan Systems Pyongyang also regularly received funds from the Korea Mining Development Trading Corporation (KOMID)[39].

[37] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 34
[38] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 34
[39] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 36

Pan Systems Pyongyang network



Source: Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 36.

Financial operations of Glocom/Pan Systems Pyongyang

In its banking operations, Pan Systems Pyongyang and its front companies used an extensive network of individuals, companies and offshore bank accounts to procure and market arms and related materiel. The global network consisted of individuals, companies and bank accounts in China, Indonesia, Malaysia, Singapore and the Middle East. In particular, €36,939 was transferred to International Global Systems in 2008 from an account at the Damascus branch of a Middle Eastern bank[40].

Since 1998, Pan Systems Pyongyang and International Global Systems have used accounts in United States dollars and euros at Daedong Credit Bank (a DPRK Bank) to gain access to the international financial system, including through bank accounts in China. These accounts were used to transfer funds to a supply chain of more than 20 companies located primarily on the Chinese mainland, in Hong Kong, China, and in Singapore. In recent years, procurement shifted almost entirely to companies in China and Hong Kong, China. Most of these companies supplied electronic products, radio components and casings consistent with Glocom's advertised military communications equipment, while others were transport companies. The network also made regular transfers to various facilitators with Chinese, Korean, foreign and code names working in China, Indonesia, Malaysia and the Middle East[41].

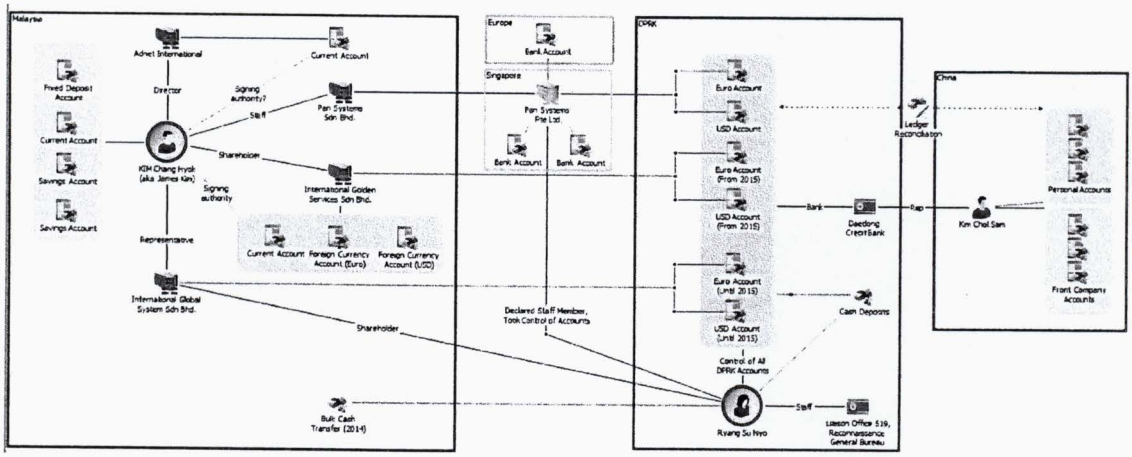
In terms of incoming transfers, Pan Systems Pyongyang received large remittances from an account at a major bank in Malaysia, as well as from numerous companies of the DPRK. Transfers were also

[40] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 77
[41] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 77

made from the Shenyang consulate of the DPRK. Pan Systems Pyongyang also regularly used bulk cash transfers. In addition, Pan Systems Pyongyang received funds from two designated entities, KOMID and Hyoksin Trading Corporation. Between 2011 and 2013, Hyoksin made multiple euro denominated transfers to Pan Systems Pyongyang, as did KOMID between 2011 and 2015[42].

In addition to its four bank accounts with the Daedong Credit Bank in Pyongyang, the Glocom network controlled at least 10 accounts in four other countries between 2012 and 2017, including through Malaysia-based front companies. Records show that these multiple overseas accounts allowed Glocom to continuously move funds between accounts it controlled in different banks and countries in the course of its illicit trade[43].

Accounts controlled by Glocom



Source: Report of the Panel of Experts pursuant UNSCR 1874, S/2018/171, p. 64

[42] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 78
[43] Report of the Panel of Experts pursuant UNSCR 1874, S/2018/171, p. 64

References

Financial Action Task Force, February 2015. *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL),* Paris: FATF.

Financial Action Task Force, October 2013. *The Role of Hawala and Oter Similar Service Providers in Money Laundering and Terrorist Financing,* Paris: FATF.

Financial Action Task Force, October 2015. *Emerging Terrorist Financing Risks,* Paris: FATF.

Panel of Experts pursuant to UNSCR 1874, S/2020/151. *Report of the Panel of Experts established pursuant to UNSCR 1874,* New York: United Nations Security Council.

Panel of Experts pursuant UNSCR 1874, S/2017/150. *Report of the Panel of Experts established pursuant to resolution 1874,* New York: United Nations Security Council.

Panel of Experts pursuant UNSCR 1874, S/2018/171. *Report of the Panel of Experts pursuant UNSCR 1874,* New York: United Nations Security Council.

Panel of Experts pursuant UNSCR 1874, S/2019/171. *Panel of Experts Report Pursuant UNSCR 1874 S/2019/171,* New York: United Nations Security Council.

Panel of Experts pursuant UNSCR 1874, S/2019/691. *Report of the Panel of Experts established pursuant to resolution 1874 (2009),* New York: United Nations Security Council.

United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015), S/2020/493. *The joint report of the Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015),* New York: United Nations Security Council.

United Nations Office on Drugs and Crime, 2012. *The Use of the Internet for Terrorist Purposes,* New York: UNODC.

www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware, 2018. *FASTCash: How the Lazarus Group is emptying millions from ATMs..* [Online]
Available at: www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware.