التدفقات المالية غير المشروعة الناجمة عن الاحتيال الذي يسهل الإنترنت ارتكابها

تشرين الثاني/نوفمبر 2023

مجموعة العمل المالي (فاتف) هي هيئة مستقلة مشتركة بين الحكومات تضع وتعزز سياسات لحماية النظام المالي العالمي من غسل الأموال وتمويل الإرهاب وتمويل انتشار أسلحة الدمار الشامل. وتوصيات مجموعة العمل المالي معترف بها على أنها المعيار العالمي لمكافحة غسل الأموال وتمويل الإرهاب. لمزيد من المعلومات حول مجموعة العمل المالي، يرجى زيارة الموقع الإلكتروني: **www.fatf-gafi.org**. لا تخلّ هذه الوثيقة و/أو أي خريطة مدرجة فيها بوضع أو سيادة أي إقليم، ولا بترسيم الحدود والتخوم الدولية ولا باسم أي إقليم أو مدينة أو منطقة.

تهدف مجموعة إيغمونت لوحدات الاستخبارات المالية (مجموعة إيغمونت) إلى توفير منتدى لوحدات الاستخبارات المالية في جميع أنحاء العالم من أجل تحسين التعاون في مجال مكافحة غسل الأموال وتمويل الإرهاب وتعزيز تنفيذ البرامج المحلية في هذا المجال. للمزيد من المعلومات عن مجموعة إيغمونت، يرجى زيارة الموقع: www.egmontgroup.org.

يتمثل دور الإنتربول في تمكين الشرطة في البلدان الأعضاء البالغ عددها 195 بلدًا من العمل معًا لمكافحة الجريمة العابرة للحدود الوطنية وجعل العالم مكانًا أكثر أمنًا. ويمتلك الإنتربول قواعد بيانات عالمية تحتوي على معلومات الشرطة عن المجرمين والجريمة، ويقدم الدعم التشغيلي وخدمات الطب الشرعي والتحليل والتدريب. وتتاح هذه القدرات الأمنية على مستوى العالم وتدعم ثلاثة برامج عالمية: مكافحة الإرهاب والجريمة السيبرانية والجريمة المنظّمة والناشئة.

المرجع:

(*التدفّقات المالية غير المشروعة الناجمة عن الاحتيال الذي يسهّل الإنترنت ارتكابه*، مجموعة العمل المالي – الإنتربول – مجموعة إيغمونت، باريس، فرنسا www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html 2023)

FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France

(فاكس: 37 61 30 44 1 33+ أو البريد الإلكتروني: contact@fatf-gafi.org)

المحتويات

قائمة الأسماء المختصرة

AML/CFT	مكافحة غسل الأموال وتمويل الإرهاب
ATM	الصراف الآلي
BEC	اختراق البريد الإلكتروني التجاري
CDD	العناية الواجبة تجاه العملاء
CEF	الاحتيال الذي يسهّل الإنترنت ارتكابه
DNFBP	الأعمال أو المهن غير المالية المحددة
FI	المؤسسات المالية
FIU	وحدة استخبارات مالية
IBAN	رقم الحساب المصرفي الدولي
IP	بروتوكول الإنترنت
LEA	وكالة إنفاذ القانون
ML	غسل الأموال
MLA	المساعدة القانونية المتبادلة
PSP	مزود خدمة الدفع
PPP	الشراكة بين القطاعين العام والخاص
STR	تقرير المعاملات المشبوهة
TF	تمويل الإرهاب
TBML	غسل الأموال القائم على التجارة
VA	أصول افتراضية
VASP	مزوّد خدمة الأصول الافتراضية
vIBAN	رقم الحساب المصرفي الدولي الافتراضي
VPN	شبكة خاصة افتراضية
VoIP	نقل الصوت على بروتوكول الإنترنت

الملخص التنفيذي

الاحتيال الذي يسهّل الإنترنت ارتكابه (CEF) هو جريمةٌ منظّمةٌ متناميةٌ عابرةٌ للحدود الوطنية. وكثيرًا ما تكون العصابات الإجرامية المقترفة للاحتيال الذي يسهّل الإنترنت جيّدة التنظيم، فتدخل في جماعات فرعية، تتميز كل واحدة عن الأخرى، ولكل واحدة منها اختصاص إجرامي، ومن ذلك غسل الأموال. وقد تكون هذه المجموعات الفرعية أيضًا فضفاضة التنظيم، وغير مركزية، وعابرة لحدود ولايات قضائية مختلفة، وهذا يزيد عرقلة الجهود المبذولة للتحقيق في نشاط الاحتيال الذي يسهّل الإنترنت ارتكابه. وتبيَّن أيضًا أن عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه متصلةٌ بصنوف أخرى من الإجرام، ولا سيّما الاتّجار بالبشر والسّخرة في مراكز الاتصال التي يجري فيها الاحتيال الذي يسهّل الإنترنت ارتكابه، إضافةً إلى تمويل انتشار التسلح المرتبط بالأنشطة الإلكترونية غير المشروعة الآتية من جمهورية كوريا الشعبية الديمقراطية.

وتشارك مجموعات غسل الأموال مع ميسّرين محترفين في عملية غسل الأموال المرتبط بالاحتيال الذي يسهّل الإنترنت ارتكابه. وصحيح أن شبكة حسابات غسل الأموال تتضمّن عادةً بغال المال (money mules)، ولكن يمكن أن تتضمّن أيضًا شركات صورية أو أعمالاً تجاريةً مشروعة. وتحتوي شبكات غسل الأموال أيضًا على أنواع مختلفة من المؤسسات المالية، بما في ذلك البنوك ومزوّدو خدمات الدفع وتحويل الأموال، ومزوّدو خدمات الأصول الافتراضية (VASPs). ويستخدم المجرمون لإخفاء المسار المالي لمكاسبهم غير المشروعة مجموعة من مختلف تقنيات غسل الأموال، مثل استخدام النقد وغسل الأموال القائم على التجارة (TBML) والخدمات غير المرخصة.

وبمساعدة الرقمنة، أتاحت التكنولوجيا لمجرمي الاحتيال الذي يسهّل الإنترنت ارتكابه تطويرَ أنشطتهم غير المشروعة وتوسيع رقعتها ونطاقها وزيادة سرعتها. فهم يستخدمون أدوات وتقنيات شتّى لخداع الضحايا أو استغلال حالتهم النفسية وعواطفهم لانتزاع أكبر قدر ممكن من الأموال. وتستغل عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه التطوُّرات التكنولوجية لتسهيل غسل متحصلات جرائمها وتسريع ذلك. كما أن الخدمات الافتراضية، كخدمة فتح الحساب عن بعد عبر الإنترنت، تسمح للمجرمين بإنشاء حسابات أجنبية وغسل المتحصلات في الخارج بسهولة، مع تنفيذ المعاملات المالية بسرعة تكاد تكون فورية. ويستغل المجرمون وسائل التواصل الاجتماعي ومنصات المراسلة في تعيين واستخدام بغال المال عبر الحدود على نطاق واسع. كما يسارع المجرمون أيضًا إلى استغلال نقاط الضعف التي تظهر من خلال المؤسسات والمنتجات المالية الرقمية الجديدة، وكذلك في القطاعات غير التقليدية مثل التجارة الإلكترونية ووسائل التواصل الاجتماعي ومنصات البث المباشر.

ويتعين على الولايات القضائية أن تستجيب استجابةً أكثر فعّالية. لذلك عليها:

- أن تستخدم مبادرات لزيادة الإبلاغ عن الضحايا وتعزيز الإبلاغ عن المعاملات المشبوهة،
- وأن تحلّل تحليلاً فعّالاً تدفقات المعلومات الوافرة للتصدّي للاحتيال الذي يسهّل الإنترنت ارتكابه،
- وأن تعي أنه نظرًا إلى الطبيعة الشاملة للاحتيال الذي يسهّل الإنترنت ارتكابه، هناك حاجة إلى تبنّي آليات تنسيق محلية قوية لمكافحة ومنع الاحتيال الذي يسهّل الإنترنت ارتكابه وما يتصل به من غسل الأموال مكافحةً ومنعًا شاملَين.

هذا وإنّ الموقع الذي تحدث فيه الجرائم الأصلية للاحتيال الذي يسهّل الإنترنت ارتكابه يميل إلى أن يكون مختلفًا عن الموقع الذي يحدث فيه غسل الأموال. فغسل المتحصلات يمكن أن يكون سريعًا من خلال شبكة من الحسابات، وهي غالبًا ما تمتدُّ عبر ولايات قضائية ومؤسّسات مالية متعددة. ولذلك يجب أن تتعاون الولايات القضائية تعاوُنًا متعدّد الأطراف من أجل تفعيل وتسريع اعتراض المتحصلات المتأتية عن الاحتيال الذي يسهّل الإنترنت ارتكابه التي يتم غسلها عبر الحدود. ولفعل ذلك، ينبغي للولايات القضائية أن تعزّز وتدعم الآليات المتعددة الأطراف القائمة بالفعل (وأيّ آلية مستقبلية) (مثل آلية الإنتربول لوقف المدفوعات I-GRIP ومشروع مجموعة إيغمونت المسمّى: الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال)، وذلك للتعاون الدولي السريع وتبادل المعلومات لمكافحة الاحتيال الذي يسهّل الإنترنت ارتكابه مكافحةً أكثر فعالية.

وأخيرًا، يورد التقرير قائمةً بمؤشرات المخاطر، إضافةً إلى متطلبات وضوابطَ مفيدةً لمكافحة الاحتيال، والتي قد تكون مفيدةً لهيئات القطاعين العام والخاص في كشف ومنع الاحتيال الذي يسهّل الإنترنت ارتكابه وما يتعلق به من غسل الأموال.

1. مقدمة

1. سيطر الاحتيال والخداع عبر الإنترنت على مشهد الجرائم التي يسهّل الإنترنت ارتكابها (cyber-enabled). وإذا لم يتم التصدي لها، فإنه سيتنامى تطوُّرها وتمرُّسها وسيكبر خطرها وتهديدها، إذ سينخرط في هذا النشاط غير المشروع مزيد من جماعات الجريمة المنظّمة وسيستفيدون من الفرص التي توفرها التقانات الجديدة، مثل الذكاء الاصطناعي التوليدي.[1]

2. وقد بدأت مجموعة العمل المالي (فاتف)، برئاسة سنغافورة، مبادرةً جديدةً للتركيز على مكافحة التدفقات المالية غير المشروعة الناجمة عن الاحتيال الذي يسهّل الإنترنت ارتكابه. وهذا التقرير هو نتيجة مشروعٍ مشترك بين مجموعة إيغمونت ومجموعة العمل المالي والإنتربول، وهو أوّل مشروع تشترك من أجل تنفيذه هذه المنظّمات الثلاث، ويعكس هذا الاشتراك التزامًا جماعيًا قويًّا بالتصدي للمجرمين المنظّمين العابرين للحدود الوطنية وشبكاتهم.

1-1 التركيز والنطاق

3. يركز هذا التقرير على التمويل غير المشروع الناشئ عن الاحتيال الذي يُسهَّل ارتكابه من خلال البيئة السيبرانية أو ضمنها، ويدخل فيه: أولاً الإجرام العابر للحدود الوطنية مثل الجهات الفاعلة العابرة للحدود الوطنية وتدفقات الأموال العابرة للحدود الوطنية، وثانيًا تقنيات الهندسة الاجتماعية المضللة (أي التلاعب بالضحايا للحصول على المعلومات السرية أو الشخصية). ولمّا كان لهذا الاحتيال أنواع كثيرة متغايرة، ركّز هذا التقرير على الأنواع الآتية من الأنشطة الإجرامية (وأشارَ إليها مجتمعةً باسم الاحتيال الذي يسهّل الإنترنت ارتكابه (CEF)):

- **الاحتيال باختراق البريد الإلكتروني التجاري (BEC):** وهو أن يتلقى الضحايا تعليمات عبر البريد الإلكتروني يُزعَم أنها من عملائهم أو مورديهم تطلب إليهم تحويل الأموال إلى حساباتِ دفعٍ جديدة.
- **الاحتيال بالتصيُّد:** وهو أن يُخدَع الضحايا للكشف عن معلومات حساسة مثل البيانات الشخصية أو التفاصيل المصرفية أو بيانات تسجيل الدخول إلى الحساب. ثم يستخدم المجرم المعلومات لاستنزاف أموال الضحايا من حسابات الدفع الخاصة بهم، أو لفتح حسابات دفع جديدة، أو لإجراء معاملات احتيالية.
- **الاحتيال بوسائل التواصل الاجتماعي وبانتحال هوية موظفي الاتصالات:** وهو أن يتصل المجرمون بالضحايا عبر تطبيقات الهاتف المحمول أو وسائل التواصل الاجتماعي، ويدّعون أنهم موظفون حكوميون أو أقارب أو أصدقاء، ويستغلون عواطف الضحايا لحثّهم على الدفع أو لإعطائهم التحكّم بحسابات الدفع، أو للقيام بأنشطة مالية كطلب قرض أو فتح حساب لتلقي المتحصلات الإجرامية.
- **الاحتيال بالتداول عبر الإنترنت أو الاحتيال بمنصة التداول:** وهو أن يُضلَّل الضحايا من خلال إعلانات مزيفة أو مستشارين عبر الإنترنت لمنصات غير موجودة أو منصات مزيفة (احتيالية) للتداول أو الاستثمار في كلٍّ من الأصول الورقية والافتراضية.
- **الاحتيال بعلاقة غرامية عبر الإنترنت:** وهو أن يُغرَى الضحايا لإرسال أموالٍ إلى المجرمين بعد إقناعهم بأنهم في علاقة غرامية.
- **حيل التوظيف:** وهي عروض عمل مزيفة على منصات التواصل الاجتماعي تخدع الضحايا لدفع أموال للمحتالين متعللين بذرائع شتّى، منها الدفع المُقدَّم لشراء سلع لتعزيز مبيعات منصة التداول أو رسوم ضمان للحصول على الوظيفة.

4. لا يقع في نطاق هذا التقرير التمويل غير المشروع ببرمجيّات انتزاع الفدية ولا غيرها من الجرائم التي تُسهّل ارتكابها البرمجيّات الخبيثة. وينبغي للقرّاء أن يرجعوا إلى تقرير مجموعة العمل المالي المعنون بـ"مكافحة تمويل برمجيّات انتزاع الفدية (المنشور في مارس/آذار 2023)" للحصول على مزيد من المعلومات عن برمجيّات انتزاع الفدية، إضافةً إلى معلومات عن غسل الأموال من خلال الأصول الافتراضية (VA) ومزوّدي خدمات الأصول الافتراضية (VASPs)، وكذلك الاطّلاع على التحديات والممارسات الجيدة للتخفيف من المخاطر. فإنّ هذه المعلومات ذات أهمية نظرًا إلى أن الأصول الافتراضية ومزوّدي خدمات الأصول الافتراضية يُستَغَلُّونَ أحيانًا لغسل متحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه.

[1] انظر أيضًا صندوق النقد الدولي (أغسطس/آب 2023) *مذكرة التكنولوجيا المالية: الذكاء الاصطناعي التوليدي في الشؤون المالية: اعتبارات المخاطر*.

2-1 الأهداف والهيكل

5. الغرض من هذا التقرير توسيع فهم السلطات المختصة لمخاطر التهديد الناجم عن الاحتيال الذي يسهّل الإنترنت ارتكابه. والتقرير مبنيٌّ على العمل الذي قد أنجزته مجموعة العمل المالي والهيئات الدولية الأخرى (ومنها مجموعة إيغمونت، واليوروبول، والإنتربول)، ويتطلع إلى تحديد التطورات الهامّة الناشئة ذات الصلة بتوسيع الفهم للمخاطر.

- ويناقش **الفصلان الثاني والثالث** من التقرير بيئة مخاطر التشغيل الحالية المتعلقة بالاحتيال الذي يسهّل الإنترنت ارتكابه، ويقدمان أفكارًا مستنيرةً حول المخاطر والتقنيات والاتجاهات في الاحتيال الذي يسهّل الإنترنت ارتكابه وما يتصل به من غسل الأموال (ML)، ومن ذلك تأثير ونقاط ضعف الرقمنة والتقانات الجديدة.
- وأما **الفصلان الرابع والخامس** من التقرير فيحدّدان الممارسات الجيدة والحلول التشغيلية التي تستخدمها الولايات القضائية للتغلب على التحديات التي تعترض معالجة وتعطيل الاحتيال الذي يسهّل الإنترنت ارتكابه وما يتصل به من غسل الأموال، ومن ذلك الآليات المستخدمة للتعاون الدولي واسترداد الأموال.

3-1 المنهجية

6. اشترك في قيادة هذا المشروع خبراء من سنغافورة (نيابةً عن مجموعة العمل المالي)، ومن وحدة الاستخبارات المالية بهونغ كونغ في الصين (نيابةً عن مجموعة إيغمونت) ومن الإنتربول. وقد أسهم في العمل أيضًا الولايات القضائية والكيانات الآتية إذ كانت جزءًا من فريق المشروع: أذربيجان، والبرازيل، وبلجيكا، وكندا، والصين، ومجلس أوروبا، والمفوضية الأوروبية، واليوروبول، وألمانيا، وفرقة العمل المعنية بغسل الأموال في غرب إفريقيا (GIABA)، والهند، وإيطاليا، وإسرائيل، واليابان، وماليزيا، والمكسيك، ولجنة الخبراء المعنية بتقييم تدابير مكافحة غسل الأموال وتمويل الإرهاب (MONEYVAL)، وباكستان، والبرتغال، والمملكة العربية السعودية، وتوغو. والمملكة المتحدة والولايات المتحدة.

7. وتستند الاستنتاجات الواردة في التقرير:

- إلى مراجعةٍ للمؤلفات الموجودة والمواد المفتوحة المصدر الدائرة حول هذا الموضوع. ويشمل ذلك البيانات والبحوث التي أجرتها مجموعة إيغمونت والإنتربول.
- وإلى طلبٍ إلى الشبكة العالمية لمجموعة العمل المالي وإلى مجموعة إيغمونت أرسلته أكثر من 200 ولاية قضائية و170 وحدة استخبارات مالية، على الترتيب، للحصول على معلومات عن المخاطر وأُطُر التنفيذ والإستراتيجيات، وكذلك عن الآليات المستخدمة في التعاون والتنسيق المحليَّين والدوليَّين. وبالجملة، فقد تلقى فريق المشروع مُدخلاتٍ من أكثر من 80 وفدًا.
- وإلى مناقشاتٍ وأفكار أثيرت في اجتماع الخبراء المشترك لمجموعة العمل المالي (أبريل/نيسان 2023) والمنتدى الاستشاري للقطاع الخاص (مايو/أيار 2023)، ومن ذلك مشاركة محددة الأهداف مع القطاع الخاص.

2 بيئة المخاطر: الاحتيال الذي يسهّل الإنترنت ارتكابه

2-1 تزايد تهديد غسل الأموال (ML)

8. زاد الاحتيال الذي يسهّل الإنترنت ارتكابه ازديادًا عظيمًا على المستوى الدولي. ومع أنه لا يوجد تقديرٌ كامل لكثرة واتساع رقعة الاحتيال الذي يسهّل الإنترنت ارتكابه، فإن عديدًا من الولايات القضائية تشير إلى نموٍّ ثابت له في السنوات الأخيرة. وكثيرًا ما يتم تحويل المتحصلات غير المشروعة المتأتية من الاحتيال الذي يسهّل الإنترنت ارتكابه إلى ولاية قضائية أجنبية. وقد تُغسَل بعد ذلك هذه المتحصلات من خلال الأنظمة المالية في ولايات قضائية تابعة لأطراف ثالثة.

9. وقد جاء في تقرير الإنتربول عن اتجاهات الجريمة في العالم لعام 2022[2] أنّ عمليات الخداع عبر الإنترنت تعدّ أحد اتجاهات الجرائم الإلكترونية التي يُنظر إليها في كثير من الأحيان على أنها تشكّل تهديدات "عالية" أو "عالية جدًا" على مستوى العالم. وتُقِرُّ معظم الولايات القضائية التي قدمت معلومات لهذا المشروع بمخاطر غسل الأموال الناجمة عن الاحتيال الذي يسهّل الإنترنت ارتكابه، وذلك ضمن تقديرات المخاطر الوطنية الخاصة بها. ومن المتوقع أن تكون المناطق التي لا نقد فيها، المعتمدة على الرقمنة إلى حد كبير (ومثال ذلك المناطق التي يتم فيها القدر الأكبر من الوساطة المالية عبر خدمات الإنترنت) أكثرَ عرضةً لمخاطر غسل الأموال المرتبطة بهذه الجريمة، مع أنّ الطبيعة العابرة للحدود الوطنية للاحتيال الذي يسهّل الإنترنت ارتكابه تعني أنه يمكن للمجرمين استهداف الضحايا بيُسر بقطع النظر عن الحدود الدولية. ويجمع المربع أدناه مصادر مختلفة للمعلومات[3] تقدّم نظرةً عامة إقليمية عن مشهد التهديدات الناجمة عن الاحتيال الذي يسهّل الإنترنت ارتكابه.

المربع 1: ازدياد تهديدات غسل الأموال: الاتجاهات الإقليمية للاحتيال الذي يسهّل الإنترنت ارتكابه

إفريقيا: أتاح القطاع المالي المرقمن سريعًا في إفريقيا كثيرًا من الفرص للمجرمين مكّنتهم من الاحتيال الذي يسهّل الإنترنت ارتكابه، فأدّى ذلك إلى زيادة شديدة في عمليات الاحتيال المصرفي عبر الإنترنت، ومن ذلك التصيُّد، وسرقة الهوية، وعمليات الخداع في الأصول الافتراضية. فارتفعت الخسائر المالية الناجمة عن مثل هذه الجرائم فزاد تهديد غسل الأموال. ومثال ذلك أنه في غرب إفريقيا وردت تقارير تقول إن الاحتيال الذي يسهّل الإنترنت ارتكابه يُعدُّ مصدرًا رئيسًا لمتحصلات الجريمة.

الأمريكتان: قد تم تحديد الاحتيال الذي يسهّل الإنترنت ارتكابه على أنّه خطر متزايد أو ناشئ. وذكرت إحدى الولايات القضائية كيف أن تقارير الاحتيال الذي يسهّل الإنترنت ارتكابه ترتفع كل سنة أكثر فأكثر، وذكرت أن مخاطر غسل الأموال المتصلة به ستزداد بحسب ذلك. وجاء في تقرير آخر أن الاحتيال بالاستثمار في الأصول الافتراضية زاد بنسبة تزيد على 180 بالمئة بين سنتَي 2021 و2022، وأنه قد استفاد المجرمون من الضجيج الإعلامي والدعاية الدائرين حول الأصول الافتراضية.

آسيا والمحيط الهادئ: ذكرت الولايات القضائية أن الاحتيال الذي يسهّل الإنترنت ارتكابه هو تهديد مرتفع أو عظيم من تهديدات غسل الأموال. ومثال ذلك أن إحدى الولايات القضائية ذكرت أن معظم تقارير الاحتيال تحتوي على نوع من أنواع الاحتيال الذي يسهّل الإنترنت ارتكابه وأنّها لاحظت زيادةً في غسل الأموال المرتبط به. وسلطت ولاية قضائية أخرى الضوء على دور الجهات الفاعلة العابرة للحدود الوطنية في الاحتيال على الضحايا من خلال عددٍ جمٍّ من تطبيقات الاستثمار غير القانونية. وقد أدّت جائحة كوفيد-19 إلى تسريع رقمنة الخدمات المقدمة للمواطنين وتغيير سلوكهم وسلوك الحكومات والشركات في المنطقة بحسب ذلك. فاشتدّ الاحتيال الذي يسهّل الإنترنت ارتكابه وما يرتبط به من غسل الأموال، ومن المتوقع أن يستمر في الاشتداد.

البحر الكاريبي: هذه المنطقة كثيرة العُرضة للاحتيال الذي يسهّل الإنترنت ارتكابه ولما يتصل به من غسل الأموال، وقد ازداد فيها الاحتيال المتعلق بالاحتيال الذي يسهّل الإنترنت ارتكابه بالجملة على مدى السنوات الخمس الماضية. هذا وقد نجم عن قطاع الأصول الافتراضية المتنامي في حوض البحر الكاريبي نقاط ضعف، ومنها ما سبّبه وجود مزوّدي خدمات الأصول الافتراضية، كخدمة الخلط، التي

2 انظر الإنتربول (2022) اتجاهات الجريمة في العالم: تقرير موجز

3 تشتمل على معلومات وبيانات قدّمتها الولايات القضائية، وعلى تقارير من الإنتربول واليوروبول.

قد يساء استخدامها فتغسل بها الأموال غير المشروعة وتُعادُ إلى جماعات الجريمة المنظمة، ومن ذلك الاحتيال الذي يسهّل الإنترنت ارتكابه.

أوروبا: إنّ الاحتيال الذي يسهّل الإنترنت ارتكابه محدّد فيها عمومًا على أنه يُشكّل تهديدَ غسل الأموال. ولاحظت ولايات قضائية كثيرة زيادةً كبيرة في هذا النشاط، وباتت تنظر إلى الاحتيال الذي يسهّل الإنترنت ارتكابه على أنه يُشكّل تهديدات كبيرة. وقد لوحظ أن استخدام الأصول الافتراضية يكون عادةً لغسل متحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه (ولا سيّما الاحتيال بالتداول عبر الإنترنت المتعلق بالأصول الافتراضية، ومثاله: الاحتيال بالعروض الأولية للعملات الرقمية).

الشرق الأوسط وشمال إفريقيا: شهدت هذه المنطقة، كما شهد غيرها من مناطق العالم، تسارعًا في معدلات الرقمنة خلال الجائحة، إذ حوّلت الحكومات والشركات والمواطنون أكثر أنشطتهم إلى الإنترنت. وصُنّف فيها الاحتيال المالي عبر الإنترنت، ومنه التصيُّد وانتحال الشخصية والخداع عبر الإنترنت، على أنها تهديدات كبيرة. ثم إنّ منطقة الشرق الأوسط وشمال إفريقيا معرضة أيضًا لغسل الأموال، إذ إنّ دول مجلس التعاون الخليجي، على وجه الخصوص، هي مراكز نقل وشحن بين السفن، عظيمة الشأن للتجارة العالمية والأنشطة المالية.

10. إن الرقمنة وتطوير التقانات الجديدة هما محرّكان رئيسان لدعم نموّ الاحتيال الذي يسهّل الإنترنت ارتكابه. وذلك لأن الخدمات الرقمية صارت الآن جزءًا لا ينفصل من الحياة اليومية والوظائف العامّة. فنتج من ذلك أن مزيدًا من المواطنين (بما فيهم الفئات المستضعفة) أصبحوا يشاركون في النشاط عبر الإنترنت. وفي الوقت نفسه، ينتج عن الرقمنة أن الولايات القضائية أصبحت مرتبطةً ارتباطًا متزايدًا بالمعلومات والأموال التي تتحرك بسرعة عبر الحدود. وقد أدّى هذان العاملان إلى تغيير المشهد الإجرامي تغييرًا جذريًا، وأنشأ بيئةً تتزايد فيها التهديدات من الاحتيال الذي يسهّل الإنترنت ارتكابه.

11. أدّت جائحة كوفيد-19 إلى تسريع التحوُّل من الأنشطة المالية التي تجري بصفة شخصية إلى فتح الحسابات والدفع والإقراض عبر الإنترنت. وقد ازدادت الأنشطة الاحتيالية ازديادًا شديدًا، مثل عمليات الخداع عبر الهاتف والبريد الإلكتروني المتعلقة بالمصارف وكبار السن والرعاية الصحية (ومثال ذلك الاحتيال بمعدّات الوقاية الشخصية وغيرها من منتجات الرعاية الصحية) وعمليات الخداع بالاستثمار الاحتيالي، وذلك عبر الإنترنت، من خلال استخدام الهواتف الذكية والبريد الإلكتروني ووسائل التواصل الاجتماعي. وقد أثّرت هذه السلوكيات المالية المتغيّرة أيضًا على مشهد غسل الأموال، ومن ذلك زيادة استخدام الخدمات المصرفية الرقمية ومنصات الدفع والمعاملات عن بُعد (انظر أيضًا القسم المعنون بـ "تأثير الرقمنة والتقانات الجديدة" في الصفحة 24).[4]

12. وقد أدّى الاستخدام المتزايد المنتشر للهواتف الذكية والتكنولوجيا (مع الأدوات والتطبيقات الجديدة المتطورة باستمرار)، والمعاملات المالية عن بُعد، إلى زيادة كبيرة في ضعف المستخدمين. وهذا، إلى جانب التكنولوجيا المعزّزة لإخفاء الهوية، كالشبكات الخاصة الافتراضية (VPN) وموجّه البصل (The Onion Router)[5]، يمكن أن يتيح للمجرمين عباءةً يخفون بها هويتهم في أنشطتهم غير المشروعة. ويمكن للمجرمين بالاستفادة من التكنولوجيا أن يزيدوا حجم أنشطتهم الإجرامية ونطاقها وسرعتها. ولوحظ أنّ المجرمين يتبنون نموذجًا اسمه "الجريمة كخدمة"[6]، وهو ما يقلل أيضًا بشكل كبير من العراقيل التي تحول دون دخول عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه، هذا مع ازدياد التخصُّص في جوانب شتّى من الاحتيال الذي يسهّل الإنترنت ارتكابه موزعةٍ على مجموعات فرعية مختلفة (انظر القسم 2-2 أدناه).[7]

13. وفي كثير من الحالات، وسّعت الجماعات الإجرامية المنظّمة أنشطتها أو كيّفتها لتشمل الاحتيال الذي يسهّل الإنترنت ارتكابه، وذلك باستخدام التقنيات الموجودة لغسل أموالها الأخرى التي حصّلتها بشكل غير قانوني.

---

4 انظر مجموعة العمل المالي (مايو/أيار 2020) مخاطر غسل الأموال وتمويل الإرهاب المتعلقة بكوفيد-19 واستجابة السياسات لها وانظر النسخة المحدّثة منه (ديسمبر/كانون الأول 2020) نسخة محدّثة: مخاطر غسل الأموال وتمويل الإرهاب المتعلقة بكوفيد-19.

5 ويعرف أيضًا باسم "تور" (TOR)، وهو برمجية مفتوحة المصدر تسمح للمستخدمين أن يتصفحوا الإنترنت من غير كشف هويّتهم.

6 وهاهنا يقع تقسيم العمل، حيث تُطوّر الجماعات الإجرامية وتقدُّم للآخرين القدرات والمهارات والخبرات الإجرامية المتخصّصة.

7 انظر يوروبول (يوليو/تموز 2023) تقدير تهديد الجريمة المنظّمة عبر الإنترنت، وانظر أيضًا الإنتربول (2022) الجرائم المالية والسيبرية تتصدر شواغل أجهزة الشرطة في العالم وفقا لتقرير جديد للإنتربول.

المربع 2: شبكة غسل الأموال الإجرامية الشائعة المستخدمة في جرائم الاحتيال الذي يسهّل الإنترنت ارتكابه وغيرها من الجرائم

تدير شبكةٌ لغسل الأموال عمليات مقامرة عبر الإنترنت وعمليات الاحتيال الذي يسهّل الإنترنت ارتكابه في مبنى شركتها في المنطقة الاقتصادية الخاصة لدولة -أ-. ويضمّ المُجمَّع نحو عشر شركات تدير عمليات المقامرة عبر الإنترنت وعمليات الاحتيال الذي يسهّل الإنترنت ارتكابه إمّا بنفسها وإما بتأجير المساحة للآخرين للقيام بذلك. وتتضمّن الشبكة أعمالًا مشروعة مزعومة في المناطق الحدودية لدولة -ب- المجاورة، ويقود الشبكة مواطنون من دولة -ب- ويستخدمون حسابات مصرفية بعملة دولة -ب- لتيسير حركة الأموال من المنطقة الاقتصادية الخاصة إلى دولة -ج-، حيث يقيم كبار المستثمرين في الشركة. ويتم غسل الدولارات الأمريكية من المناطق الاقتصادية الخاصة من خلال مكاتب الصرافة في دولة -ب-، حيث يتم تحويل الأموال إلى عملة دولة -ب- ثم تُنقَل إلى دولة -ج-، وبعد ذلك يتم تحويل الأموال من جانب دولة -ج- من الحدود إلى مستثمري الشركة.

المصدر: الجريمة المنظمة العابرة للحدود الوطنية ونوادي القمار وغسل الأموال في جنوب شرق آسيا: تحليل التهديدات (مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2022)

2-2 الخصائص الجنائية للاحتيال الذي يسهّل الإنترنت ارتكابه

عناصر الاحتيال الذي يسهّل الإنترنت ارتكابه

14. استنادًا إلى تجارب الولايات القضائية، قد يعتمد مجرمو الاحتيال الذي يسهّل الإنترنت ارتكابه على عنصر أو أكثر من العناصر الآتية لخداع الضحايا بنجاح لإجراء تحويل احتيالي. ويمكن للمتغيّرات المختلفة للاحتيال الذي يسهّل الإنترنت ارتكابه أن تجمع بين العناصر المذكورة أعلاه بطرق شتّى.

- استخراج المعلومات (ومثاله: استخراجها بالتصيُّد).
- الخداع الاجتماعي أو الهندسة الاجتماعية، واستغلال رقّة المشاعر (ومثاله: الخداع من خلال التظاهر بأنه شخص أو كيان آخر واستخدام ذلك كمقدمة للحثّ على الاستعجال أو الخوف أو الثقة، أو الخداع من خلال تقديم ادعاءات كاذبة لكسب المال بسهولة).
- وسيلة أو منصة عبر الإنترنت (يمكن استخدامها للتواصل أو لإجراء معاملات الضحايا في حالات الاحتيال التجاري عبر الإنترنت).

15. وقد لا تقع الضحية في نوع واحد فقط من الاحتيال الذي يسهّل الإنترنت ارتكابه، فالغرض في آخر المطاف هو الحث على تحويل الأموال، ولذلك يستخدم المجرمون مجموعةً متنوعةً من التقنيات لتحقيق ذلك. والمجرمون مبدعون، فقد ينخرطون أو ينتقلون إلى أنواع أخرى من الاحتيال الذي يسهّل الإنترنت ارتكابه إذا بدأت الخدعة الأولى بالفشل. ومثال ذلك: أنه إذا وقع إنسان ضحيةً للتصيُّد الاحتيالي أو لانتحال الهوية عبر وسائل التواصل الاجتماعي فيمكن إقناعه وتوجيهه إلى مخطط احتيال استثماري من قبل المجرم نفسه الذي أوقعه أول مرة، وذلك من خلال الاستفادة من "الثقة" التي تم بناؤها بالفعل من خلال مخطط الاحتيال الأول.

المربع 3: تعددت الجرائم والضحيّة واحدة

إنّ خدعة ذبح الخنازير هي مزيج من الاحتيال بعلاقة غرامية والاحتيال بالاستثمار. وطريقة عملها أنّ المجرمين يبنون علاقة ثقة مع الضحية ويقنعونهم باستثمار مدّخراتهم في منصات احتيالية لتداول العملات المشفرة. ويتم تنفيذ هذا الاحتيال شيئًا فشيئًا مع مرور الوقت، فيؤدي ذلك إلى خسارة مبالغ كبيرة من المال.

وبعد تنفيذ عملية الاحتيال، غالبًا ما يتصل المجرمون بضحاياهم مدّعين بأنهم محامون أو وكلاء إنفاذ القانون ويعرضون المساعدة لاسترداد الأموال مقابل رسوم.

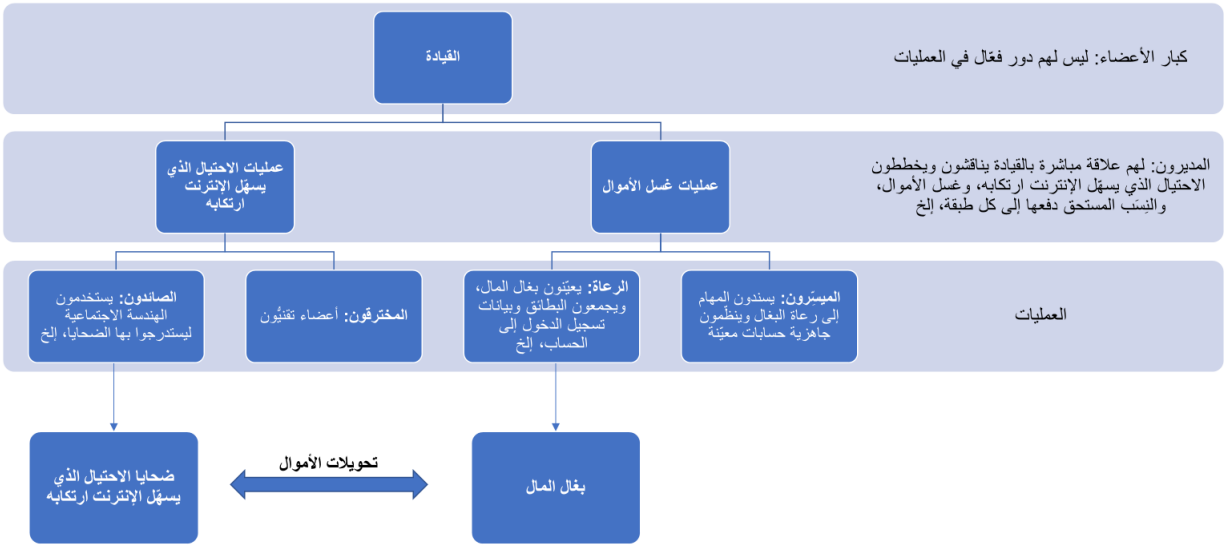
المصدر: اليوروبول (2023)، تقدير تهديد الجريمة المنظّمة عبر الإنترنت لسنة 2023

البنية الإجرامية المنظمة

16. غالبًا ما يتم تنفيذ الاحتيال الذي يسهّل الإنترنت ارتكابه وغسل الأموال المتصل به من قبل جماعات أو عصابات إجرامية منظّمة وعابرة للحدود الوطنية. ومع أنّ بنياتها قد تختلف، إلا أن عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه غالبًا ما تعمل كمنظمات هرمية (انظر مثال ذلك في الشكل 1). وقد تكون أيضًا فضفاضة التنظيم لتبقى مرنة، فينضمّ الأعضاء إليها ويغادرونها بحسب الحاجة. ويمكن أيضًا أن تُنظّم هذه العصابات على مجموعات فرعية متميز بعضها عن بعض، ذات مجالات متخصصة في الخبرة الجنائية (ومثالها: أن تتماشى مع عناصر الاحتيال الذي يسهّل الإنترنت ارتكابه المذكورة أعلاه (أي استخراج المعلومات، أو الخداع الاجتماعي، أو غيرها من الخبرات التقنية، كإنشاء منصة عبر الإنترنت أو غسل الأموال). وفي كثير من الحالات، تكون عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه هذه غير مركزية ولم تتواصل شخصيًّا البتّة (ومثال ذلك: أنها تتواصل من خلال القنوات المشفرة عبر الإنترنت)، وهذا يُصعِّبُ على السلطات التحقيق في أمرها.

17. ثم إنّ عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه تتألّف بانتظام من محترفين جيّدي التعليم وذوي كفاءة تقنية. فأفضى ذلك إلى اتّباعها لنهج متطوّر ومتمرّس بشكل متزايد في الاحتيال الذي يسهّل الإنترنت ارتكابه وغسل الأرباح غير المشروعة. ولاحظت الولايات القضائية كيف يمكن لعصابات الاحتيال الذي يسهّل الإنترنت ارتكابه أن تقوم عمدًا باستخدام أفراد يعملون في القطاعات المهنية (بما في ذلك المؤسسات المالية)، الذين يمكن الاستفادة منهم كمصادر للبيانات والمعلومات لتنفيذ الاحتيال الذي يسهّل الإنترنت ارتكابه بنجاح وتيسير غسل الأموال. ولمزيد من المعلومات حول بنية عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه وكيفية عملها في غسل الأموال، يرجى الرجوع إلى القسم 2-3 أدناه.

الشكل 1: مثال للبنية الإجرامية للاحتيال الذي يسهّل الإنترنت ارتكابه



المصدر: مجموعة العمل المالي

ارتباطات بجرائم أخرى

18. قد ترتبط عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه، إضافةً إلى غسل الأموال، بأنواع أخرى من الإجرام. وتشمل الجرائم الشائعة الأنشطة المرتبطة بالاحتيال الذي يسهّل الإنترنت ارتكابه أو الضرورية لتنفيذه، بما في ذلك أنشطة الجرائم الإلكترونية كالقرصنة للحصول على معلومات شخصية، وتطوير البرمجيات الإجرامية وبيعها، وتزوير الوثائق، وما إلى ذلك. ويمكن أن تغسل عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه جزءًا من المتحصلات الإجرامية بنفسها، وذلك لشراء معدات جديدة وتطوير أدوات تكنولوجية أكثر تقدمًا.

المربع 4: عملية الصقر

اعتُقل ثلاثة مشتبه بهم في لاغوس بنيجيريا سنة 2020 بعد تحقيق مشترك في الجرائم الإلكترونية بين الإنتربول وشركة غروب آي بي (Group-IB) وبين جهاز الشرطة النيجيرية. وقد اشتُبه في انتماء هؤلاء المواطنين النيجيريين إلى مجموعة إجرامية منظمة واسعة مسؤولة عن بثّ برمجيات خبيثة وشنّ حملات تصيّد احتيالي وارتكاب عدد كبير من عمليات الاحتيال باختراق البريد الإلكتروني التجاري. واعتُقد أن المشتبه فيهم جهزوا روابط للتصيّد الاحتيالي وأسماء نطاقات لهذا الغرض ونفذوا حملات توجيه رسائل إلكترونية بالجملة انتحلوا فيها هوية ممثلين عن بعض المنظّمات. ثم استغلوا هذه الحملات لنشر 26 برنامجًا يحتوي على برمجيات خبيثة وبرمجيات تجسُّس وأدوات تحكّم في الأجهزة عن بُعد وبرمجيات أحصنة طروادة خبيثة

واستُخدمت هذه البرامج بهدف التسلُّل إلى النظم الحاسوبية لدى المنظمات والأفراد الضحايا ومراقبتها قبل الشروع في عمليات الاحتيال واختلاس الأموال. ووفقًا لشركة Group-IB، يُعتقد أن هذه العصابة الناشطة قد ألحقت الضرر بشركات حكومية وخاصة في أكثر من 150 بلدًا منذ سنة 2017. وأثبتت شركة Group-IB أيضا أن هذه العصابة تنقسم إلى مجموعات فرعية لا يزال عدد من أفرادها أحرارًا.

وكشفت التحقيقات الموازية في غسل الأموال أن المشتبه بهم استخدموا أيضًا حسابات البنوك الأجنبية وحسابات أصول افتراضية في المملكة المتحدة والولايات المتحدة وتايلاند لتلقي الدفعات من الضحايا. فاتُّهم المشتبه بهم الثلاثة لأنشطتهم غير القانونية، بما في ذلك الاحتيال وغسل الأموال. وصودرت سيارة فاخرة وجُمِّدت حسابات المشتبه بهم ويجري مصادرة أموال هذه الحسابات في المحكمة.

المصدر: نيجيريا

19. هناك أيضًا صلة متزايدة بين الاحتيال الذي يسهّل الإنترنت ارتكابه وبين الاتّجار بالبشر، إذ يتم استدراج الضحايا من خلال إعلانات الوظائف المزيفة إلى مراكز الاتصال عبر الإنترنت وإجبارهم على اقتراف الاحتيال الذي يسهّل الإنترنت ارتكابه في المجال الصناعي. وتتيح هذه الصلة لعصابات الاحتيال الذي يسهّل الإنترنت ارتكابه زيادة التنوُّع الجغرافي لضحايا الإنترنت الذين يمكنهم استهدافهم (إذ إنّه يمكن استغلال الضحايا الذين يتم الاتّجار بهم من خلال معارفهم اللغوية وبصيرتهم الثقافية). ويمكنها أيضًا أن تزيد مراكز الاحتيال الذي يسهّل الإنترنت ارتكابه تطوُّرًا وتمرُّسًا من خلال الاتّجار بالمهنيين المهرة، مثل العاملين في مجال تكنولوجيا المعلومات أو "مديري المبيعات الرقمية".[8] إذ تتعمد مراكز الاتصال هذه أحيانًا أن تعمل ضمن المناطق الزمنية التي يعيش فيها ضحاياها المقصودون، وتستخدم العقارات المستأجرة لعمليات إجرامية مؤقتة، وهذا يسمح لها بإعادة تحديد عناوين بروتوكول الإنترنت (IP) وتغييرها بسرعة لتجنُّب أن تكشفها جهات إنفاذ القانون.[9]

المربع 5: عملية العاصفات (Operation Storm Makers)

شهدت عملية العاصفات قيام السلطات بتنفيذ إجراءات إنفاذ ضد مجموعات الجريمة المنظّمة التي يعتقد أنها تيسّر سفر الرجال والنساء والأطفال الآسيويين عبر الحدود للاستغلال أو الربح أو كليهما معًا. وأدّت العملية إلى اعتقال 121 شخصًا في 25 بلدًا، وفتح 193 تحقيقًا جديدًا.

وفي عملية العاصفات، عملت الشرطة في ماليزيا وكمبوديا عن كثب في قضية تتعلق بـ15 رجلاً وامرأة استدرجوا إلى كمبوديا على وعدٍ براتبٍ مربح مقابل العمل في مركز اتصال. ولكنهم حبسوا عند وصولهم وأجبروا على العمل 14 ساعة في اليوم كمحتالين.

ملحوظة: لمزيد من المعلومات، انظر الإنتربول (مايو/أيار 2022) اعتقال 121 شخصا في سياق عملية نسّقها الإنتربول لمكافحة تهريب المهاجرين والاتجار بالبشر

المصدر: الإنتربول

8 انظر الإنتربول (يونيو/حزيران 2023) الإنتربول يُصدر تحذيرا عالميا بشأن الاحتيال الذي يُذكي نارَه الاتجار بالبشر

9 انظر الإنتربول (يوليو/تموز 2023) تحليل ميداني: الاحتيال عبر الإنترنت والاتّجار بالبشر في جنوب شرق آسيا / التحديث الثاني: من التهديد الإقليمي إلى التهديد العالمي. وهو غير متاح إلا لسلطات إنفاذ القانون الوطنية.

20. لم تشهد معظم الولايات القضائية أدلة كافية على أنشطة تمويل الإرهاب المرتبطة بالاحتيال الذي يسهّل الإنترنت ارتكابه. ومع ذلك، كانت هناك بعض الملاحظات التي ظهر فيها ارتباط عناصر الأنشطة الإرهابية وتمويل الإرهاب بالمجرمين الذين يقترفون الاحتيال الذي يسهّل الإنترنت ارتكابه. ومثال ذلك أن تقارير عن المعاملات المشبوهة من إحدى الولايات القضائية أشارت إلى أن متحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه تم تحويلها في بعض الحالات إلى مناطق صراع معينة أو ولايات قضائية معيّنة معروفة بالأنشطة المتعلقة بالإرهاب.

21. هناك أيضًا ارتباطات بتمويل انتشار التسلح، إذ تم الإبلاغ عن الجرائم الإلكترونية باعتبارها مصدرًا رئيسيًا لتوليد الدخل غير المشروع في جمهورية كوريا الشعبية الديمقراطية. ومن الأنشطة الإلكترونية غير المشروعة بيعُ المعلومات الشخصية التي تم حصدها، أو توفير أدوات وخدمات القرصنة والتصيُّد الاحتيالي، التي يمكن أن يستخدمها مجرمون آخرون لاقتراف الاحتيال الذي يسهّل الإنترنت ارتكابه.[10]

[10] انظر أيضًا مجلس الأمن التابع للأمم المتحدة (مارس/آذار 2023) (S/2023/171) رسالة مؤرخة بـ3 آذار/مارس 2023 من فريق الخبراء المنشأ عملاً بالقرار 1874 (2009) إلى رئيس مجلس الأمن

المربع 6: استخدام أدوات التصيُّد الاحتيالي لجمهورية كوريا الشعبية الديمقراطية للاحتيال الذي يسهّل الإنترنت ارتكابه من أجل تمويل برامج الأسلحة

استنادًا إلى المعلومات التي قدمها فريق الخبراء التابع للأمم المتحدة، كان العاملون في مجال تكنولوجيا المعلومات في جمهورية كوريا الشعبية الديمقراطية المرتبطون بإدارة صناعة الذخائر يكسبون العملات الأجنبية عن طريق بيع تطبيقات التصيُّد الصوتي والقرصنة وتشغيل عديد من الخوادم وعناوين بروتوكول الإنترنت من خارج البلاد.

وفي يوليو/تموز سنة 2020، اعتقلت السلطات في الصين أربعة مواطنين من جمهورية كوريا وسلّمتهم إليها. وشهد أحدهم أن الجماعات الإجرامية اشترت معلومات شخصية لمواطني جمهورية كوريا إضافةً إلى تطبيقات التصيُّد الصوتي والقرصنة من أحد العاملين في مجال تكنولوجيا المعلومات في جمهورية كوريا الشعبية الديمقراطية.

وقد خدعت الجماعات الإجرامية الضحايا واستدرجتهم إلى تنزيل هذه الأدوات المطورة في أجهزتهم لتسرق منهم مزيدًا من المعلومات. وقد ادّعوا بعد ذلك أنهم موظفون في مؤسسة مالية ليخدعوا الضحايا حتى يرسلوا الأموال.

ملحوظة: لمزيد من التفاصيل، انظر مجلس الأمن التابع للأمم المتحدة (سبتمبر/أيلول 2022) (S/2022/668) رسالة مؤرخة 2 سبتمبر/أيلول 2022 من فريق الخبراء المنشأ عملاً بالقرار 1874 (2009) إلى رئيس مجلس الأمن

المصدر: فريق الخبراء التابع للأمم المتحدة وكوريا الجنوبية

3-2 تقنيات غسل الأموال وتطبيقاته

بنية شبكات غسل الأموال

22. عندما يغسل المجرمون المتحصلات المتأتية عن أنواع مختلفة من الاحتيال الذي يسهّل الإنترنت ارتكابه، فإنهم يجب أن يكونوا سريعين وفعّالين. ولاحظت الولايات القضائية مشاركة جماعات من المهنيين في مجال غسل الأموال إضافةً إلى ميسّرين محترفين تابعين لأطراف ثالثة، ومنهم المحامون والمحاسبون ومستشارو الضرائب وأمناء الشركات والمصرفيون. وقد تكون الجماعات المهنية لغسل الأموال جزءًا من عصابة إجرامية للاحتيال الذي يسهّل الإنترنت ارتكابه، أو قد تكون منظّمة غير مركزية منفصلة تقدم خدمات غسل الأموال تحت نموذج "الجريمة كخدمة" (أي شبكات غسل الأموال الاحترافية).

المربع 7: شبكة QQAAZZ

أعلنت شبكة QQAAZZ عن خدماتها باعتبارها "خدمة إسقاط مصرفي عالمية ومتواطئة" في منتديات الجرائم الإلكترونية عبر الإنترنت الناطقة بالروسية، حيث يجتمع مجرمو الإنترنت ويقدّمون أو يبحثون عن المهارات والخدمات المتخصّصة اللازمة للمشاركة في ضروب شتّى من أنشطة الجرائم الإلكترونية. وقامت شبكة QQAAZZ بفتح وإدارة مئاتٍ من حسابات الشركات الصورية والحسابات المصرفية الشخصية في المؤسسات المالية في جميع أنحاء العالم، وهي حسابات تم استخدامها لتلقي الأموال من مجرمي الإنترنت المقترفين للاحتيال الذي يسهّل الإنترنت ارتكابه. وبعد ذلك تم تحويل الأموال إلى حسابات مصرفية أخرى تسيطر عليها QQAAZZ، وفي بعض الأحيان تم تحويلها إلى عملة رقمية باستخدام خدمات التقليب (tumbling) التي صممت لغرض إخفاء المصدر الأصلي للأموال. وبعد أن حصّلت شبكة QQAAZZ رسومًا تصل إلى 50 بالمائة، أعادت رصيد الأموال المسروقة إلى عملائها المجرمين.

وفي نوفمبر/تشرين الثاني من سنة 2020، أسفرت عملية دولية لإنفاذ القانون شارك فيها 16 بلدًا عن اعتقال 20 شخصًا يشتبه بانتمائهم إلى شبكة QQAAZZ الإجرامية، التي حاولت غسل عشرات الملايين من اليوروهات نيابةً عن أهم مجرمي الإنترنت في العالم. وقد أجريت حوالي 40 عملية تفتيش للمنازل في لاتفيا وبلغاريا والمملكة المتحدة وإسبانيا وإيطاليا، مع بدء إجراءات جنائية ضد من اعتقلتهم الولايات المتحدة والبرتغال والمملكة المتحدة وإسبانيا.

المصدر: البرتغال واليوروبول

23. يتم عادةً غسل متحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه بسرعة من خلال شبكة من الحسابات. وتُظهر دراسات الحالة أن هذه الشبكات يمكن أن تكون معقّدة لأنها ممتدّة عبر حدودٍ ومؤسساتٍ مالية متعددة، ولكنّ ذلك قد يختلف بناءً على مستوى تطوُّر الجماعة الإجرامية وتمرُّسها.[11]

24. تتضمن عادةً شبكات غسل الأموال المتعلقة بالاحتيال الذي يسهّل الإنترنت ارتكابه أفرادًا وكيانات قانونية.

- فكثيرًا ما يقوم المجرمون بتعيين واستخدام بغال المال المنفردين بوسائل شتّى، منها بعروض العمل والإعلانات، وبالتفاعلات عبر وسائل التواصل الاجتماعي. ويُعرف القائمون على تعيين واستخدام بغال المال أيضًا باسم "رُعاة" البغال. وقد تكون بغال المال متواطئةً عن عمدٍ في غسل الأموال أو عن غير قصدٍ (من خلال الخداع)، أو عن إهمالٍ، وقد يُعرَض عليهم أيضًا حوافز أو رسوم للتعامل مع الأموال غير المشروعة. ومن الصعب تحديد هوية المتحكم في البغل (أي راعي البغل)، الذي يقوم بتعيين واستخدام المشاركين المتواطئين وغير المتعمدين، أو بتحديد مصدر أموال الاحتيال. ولاحظت بعض الولايات القضائية حالات تعيين واستخدام لمواطنين أجانب ليس لهم أيّ صلة واضحة بالولاية القضائية، إذ تم توجيه هؤلاء الأفراد لإنشاء حسابات غير مباشرة، إما عن طريق السفر الفعلي أو من خلال فتح حساب افتراضي.

11 لمزيد من المعلومات عن استعمال بغال المال عند محترفي غسل الأموال وشبكاته، انظر مجموعة العمل المالي (يوليو/تموز 2018) غسل الأموال المحترف

المربع 8: تعيين واستخدام البغال: عرض العمل

السيدة (ر س) هي صاحبة متجر صغير للسلع المتنوعة، عيّنها السيد (أو) في ما ظنّت أنه عرضُ عملٍ مشروع. والسيد (أو) هو مواطنٌ نيجيري تم القبض عليه سنة 2019 بتهمة قيامه بتنفيذ عملية احتيال بعلاقة غرامية عبر الإنترنت بملايين الدولارات، وأدّت العملية إلى خسائر تزيد على 8 ملايين بيزو فلبّيني (أي نحو 129,000 يورو).

وقد وعد السيد (أو) السيدة (ر س) بحصةٍ مقابل كل معاملة مصرفية تتناولها. وبالجملة، قامت السيدة (ر س) بمعالجة 83 معاملة بقيمة 3.6 مليون بيزو فلبّيني (أي نحو 58,000 يورو) على مدى ستة أشهر. وكانت جميع المعاملات تعتمد على النقد (أي الودائع النقدية وأجهزة الصراف الآلي والسحوبات النقدية التي تجري من كوّة المصرف). واعتُقل السيد (أو) أخيرًا بالتعاون مع السيدة (ر س) عبر عملية دُبّرت للإيقاع به.

المصدر: الفلبين

- يسيطر عادةً مجرمو الاحتيال الذي يسهّل الإنترنت ارتكابه على **الشركات الصورية** من خلال مُلّاك وهميين (strawmen) أو مديرين معيّنين. وقد يُطلب أيضًا من بغال المال الأفراد المستخدَمين أن يتصرفوا مثل أولئك، وأن يفتحوا حسابات شركات في محاولةٍ لإحداث مزيد من التعتيم على ملكية المجرم الحقيقي. ولاحظت بعض الولايات القضائية أن الشركات الصورية تستخدم عناوين تجارة افتراضية[12] لتزيد من التعتيم على أنشطتها الإجرامية. وربما استخدم المجرمون أيضًا، في حالات الاحتيال التجاري عبر الإنترنت، هذه الشركات الصورية لفتح حسابات لنقاط بيعٍ افتراضية مع شركات خدمات تجارية يعالجون بها الدفعات والتحويلات الآتية الضحايا.

12 عناوين التجارة الافتراضية هي عناوين فعلية حقيقية يقدمها بعض مزوّدي الخدمة، تسمح للشركات بتلقي البريد والطرود.

المربع 9: الشركات الصورية في الاحتيال بمنصة التداول عبر الإنترنت

تم تقديم عدد من التقارير عن المعاملات المشبوهة إلى وحدة الاستخبارات المالية في تركيا تُخبِرُ بمخطّط احتيال على منصةٍ للتداول عبر الإنترنت، اتصل أصحابها بالضحايا يعرضون عليهم الاستثمار في العملات الأجنبية عبر الهاتف أو وسائل التواصل الاجتماعي. وكان أساس هذا المخطّط عبارة عن شبكة مكونة من 209 شركات قامت بغسل المتحصلات فيما بينها. وكان عند هذه الشركات محاسبون مشتركون، وقد أُسِّست معظمها في التاريخ نفسه ثم تم تصفيتها بعد مدة وجيزة.

وكشف تحليل أجرته وحدة الاستخبارات المالية في تركيا أن الشركات الصورية عملت أيضًا في ثلاث مجموعات فرعية منفصلة، وذلك بناءً على تحويلات الأموال والشركاء الأفراد من الأطراف الثالثة المرتبطين بها. وظهر أنه تم الحصول على ما يقرب من 10 مليارات ليرة تركية (أي نحو 336.7 مليون يورو) عن طريق الاحتيال.

- تلقّت 135 شركة 9.6 مليار ليرة تركية (أي نحو 323.2 مليون يورو) من متحصلات الاحتيال من خلال شركات الدفع. ولتيسير تلقّي المعاملات من الضحايا، أنشأت هذه الشركات حسابات افتراضية لنقاط البيع. وسُحِبت 100 مليون ليرة تركية (أي نحو 3.4 مليون يورو) نقدًا، وتم تحويل نحو 6 مليارات ليرة تركية (أي نحو 202 مليون يورو) إلى إحدى شركات الذهب.
- تلقّت 59 شركة 700 مليون ليرة تركية (أي نحو 23.6 مليون يورو) من متحصلات الاحتيال. وسُحِبت 200 مليون ليرة تركية (أي نحو 6.7 مليون يورو) نقدًا، وتم تحويل المبالغ الأخرى إلى مزوّدي خدمات الأصول الافتراضية بعد غسلها من خلال حسابات يحتفظ بها شركاء أفراد من أطراف ثالثة.
- تلقّت 23 شركة 875 مليون ليرة تركية (أي نحو 29.5 مليون يورو) من متحصلات الاحتيال. وسُحِبت 220 مليون ليرة تركية (أي نحو 7.4 مليون يورو) نقدًا، وتم تحويل المبالغ الأخرى إلى مزوّدي خدمات الأصول الافتراضية بعد غسلها من خلال حسابات يحتفظ بها شركاء أفراد من أطراف ثالثة.

المصدر: تركيا

- يمكن أيضًا خداع **الشركات المشروعة**، كما يُخدَع بغال المال الأفراد، لتلقي متحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه (ومثال ذلك: الخداع بالاستثمار أو بفرصة عمل)، فيُطلَب منها إما إعادة توجيه الأموال أو ردّها إلى حساب منفصل يخضع لرقابة جنائية. وفي بعض الحالات، لوحظ أن الشركات الشرعية تقبل عن طيب خاطر هذه "الفرص التجارية" ولا سيّما في أوقات الضائقة الاقتصادية. ويتيح إشراك الشركات المشروعة واجهةً إضافيةً لإخفاء الأنشطة غير المشروعة ومنع كشفها.

25. هناك أوجه تشابه في كيفية تهيئة بغال المال في شبكات غسل الأموال من أجل الاحتيال الذي يسهّل الإنترنت ارتكابه ومن أجل أنواع أخرى من الجرائم. على أنه لاحظت الولايات القضائية بعض الاختلافات التي قد تكون أوثق صلةً ببغال الاحتيال الذي يسهّل الإنترنت ارتكابه.

- **طريقة تعيينهم واستخدامهم:** من المرجح أن يتم تعيين واستخدام بغال المال للاحتيال الذي يسهّل الإنترنت ارتكابه من الإنترنت نفسه، ومن طرائق ذلك: إعلانات الوظائف من الشركات المزيفة أو رسائل البريد الإلكتروني المزعجة. وقد يستغل المجرمون أيضًا الظروف الاقتصادية ويخفون ذلك وراء فرصة عمل مشروعة للحصول على "المال السهل". وكثيرًا ما يُخدَع ضحايا الاحتيال الذي يسهّل الإنترنت ارتكابه (ومثاله الاحتيال من خلال العلاقة الغرامية) فيعملون كبغال مال. وفي بعض الحالات، يتم استخدام ضحايا الاتّجار بالبشر (كالمهاجرين غير الشرعيين أو العمال غير الشرعيين) لفتح مثل هذه الحسابات.
- **استخدام الحسابات:** تُستخدَم بغال المال المرتبطة بالاحتيال الذي يسهّل الإنترنت ارتكابه من أجل ما يملكون من حسابات لدى المؤسسات المالية، إذ يمكن استلام الأموال الاحتيالية وإرسالها بسرعة عبر طرق الدفع الإلكترونية، بدلاً من التحويلات المادية أو الودائع النقدية. ويرجع ذلك على الأرجح إلى الطريقة التي يتم الاحتيال بها على الضحايا (أي من خلال تحويلات الأموال). ونظرًا للسهولة التي توفرها الخدمات المصرفية

الرقمية في تحريك الأموال، فمن المحتمل أن يكون عند الأفراد المستهدفين بالمعاملات المتصلة بالاحتيال الذي يسهّل الإنترنت ارتكابه قليلاً من المعرفة الأساسية أو الكفاءة في الحواسيب والتكنولوجيا.

المربع 10: تحويل ضحية للاحتيال بعلاقة غرامية إلى بغل مال

بين أبريل/نيسان ومايو/أيار من سنة 2022، تلقّت امرأة مسنّة دفعتين بمبلغ أكبر من المبالغ التي كانت تتلقاها في حسابٍ مصرفي كانت فتحته في الأصل لتلقي معاش تقاعدها. وكان أحد التحويلَيْن من حساب مصرفي محلي، أما التحويل الثاني فكان من ضحية مبلّغٍ عنها من الخارج.

فكشف تحقيق لاحق أجرته السلطات السلوفاكية أن المرأة تواصلت مع أحد الأشخاص عبر وسائل التواصل الاجتماعي ووقعت فريسة لعملية احتيال بعلاقة غرامية. إذ أعطت المرأة المسنّة للمحتال بيانات تسجيل دخولها إلى الخدمة المصرفية عبر الإنترنت، ثم استُخدِم حسابها المصرفي لغسل متحصلات جريمة أخرى. وتم تحويل جزءٍ من الأموال المستلمة إلى عملة رقمية عبر منصة أجنبية لخدمات الأصول الافتراضية.

المصدر: سلوفاكيا

تقنيات غسل الأموال وتطبيقاته

26. إنّ الموقع الذي يحدث فيه الاحتيال الذي يسهّل الإنترنت ارتكابه (أي مكان وجود الضحية) يختلف في كثير من الأحيان عن الموقع الذي يحدث فيه غسل متحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه، وقد تمتد شبكات بغال المال عبر ولايات قضائية متعددة. وذلك لأن عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه تدرك أن المؤسّسات المالية أو السلطات المختصة ربما تكون قد كشفت حسابات تجري فيها أنشطة احتيالية قبل الغسل، وهو ما يؤدّي إلى اعتراض متحصلاتها الإجرامية قبل أن تصل إلى حسابات المجرمين. وقد يقوم المجرمون لتعزيز فرص نجاح عملهم بإجراء "اختبارات" ينفّذون فيها معاملات بقيمة زهيدة، حتّى يتمكنوا من تغيير وجهة الأموال إن أخفقت الاختبارات.

27. عادةً ما يعتمد نوع حساب الطبقة الأولى من التمويه المستخدم لتلقّي متحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه على نوع هذا الاحتيال لاستمرار بقاء الواجهة الشرعية. وقد لوحظ أيضًا حدوث تغييرات بمرور الوقت في نوع حساب الطبقة الأولى من التمويه. ومثال ذلك أنه في قضايا الاحتيال باختراق البريد الإلكتروني التجاري، تحولت عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه من استخدام حسابات الأفراد إلى استخدام حسابات الشركات حتى تُقلّل مخاطر كشف أفعالها.

الجدول 1: العلاقة بين نوع الاحتيال الذي يسهّل الإنترنت ارتكابه وحساب الطبقة الأولى من التمويه

نوع الاحتيال الذي يسهّل الإنترنت ارتكابه	نوع حساب الطبقة الأولى من التمويه
احتيال باختراق البريد الإلكتروني التجاري	شركة (كشركة صورية أو كشركات مسجلة حديثًا)
الاحتيال بالتصيُّد	بغال المال الأفراد
الاحتيال بوسائل التواصل الاجتماعي وبانتحال هوية موظفي الاتصالات	بغال المال الأفراد
الاحتيال بالتداول عبر الإنترنت أو الاحتيال بمنصة التداول	شركة (كشركة صورية أو كشركات مسجلة حديثًا)
الاحتيال بعلاقة غرامية عبر الإنترنت	بغال المال الأفراد
حيل التوظيف	بغال المال الأفراد

ملحوظة: يحاول هذا الجدول استخلاص بعض الاتجاهات العامة بناءً على تجربة الولايات القضائية في أنواع حسابات الطبقة الأولى من التمويه مع ما يقابلها من نوع الاحتيال الذي يسهّل الإنترنت ارتكابه. ومع ذلك، فقد لا ينطبق ما فيه على جميع الحالات.

28. بمجرد أن تنشئ عصابة الاحتيال الذي يسهّل الإنترنت ارتكابه حسابًا تتم معالجة الأموال المكتسبة بالاحتيال سريعًا حتى تدخل إلى شبكة غسل الأموال. وبعد ذلك تُموَّه الأموال بسرعة عبر سلسلة من المعاملات "العابرة" عن طريق حسابات محلية أو أجنبية يتم التحكم فيها من قبل بغال المال أو المُلّاك الوهميين أنفسهم أو من قبل عصابة الاحتيال الذي يسهّل الإنترنت ارتكابه. وفي هذه الحالة الأخيرة، يُسلِّم بغال المال البيانات المصرفية كبيانات تسجيل الدخول والبطاقات والرموز، أو يوكّلون رسميًا عصابة الاحتيال الذي يسهّل الإنترنت ارتكابه ليمكّنوها من التحكم المباشر

في الحسابات. ثم إن إشراك الميسّرين المحترفين في العملية، كأن يُشرَكوا في أثناء إنشاء التوكيل، يضفي على المعاملات جوًا من الشرعية وييسّر التعتيم على الجريمة.

29. إنّ عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه تستخدم لتعزيز تفادي الكشف والبقاء مجهولة الهوية تقنياتٍ وآليات شتّى: منها تجزئة المعاملات (smurfing)، ومنها التنقّل بين الحسابات عبر مختلف مزوّدي الخدمات المالية أو التحويلات أو الدفع، ومنها التحوُّل إلى أنواع أخرى من الأصول المالية (مثل النقود الإلكترونية[13]، والبطاقات السابقة الدفع، والأصول الافتراضية). وقد يفضي ذلك إلى إطالة الوقت اللازم لوحدات الاستخبارات المالية وجهات إنفاذ القانون للوصول إلى البيانات المالية المطلوبة عبر الحدود والقطاعات والمؤسسات، من أجل تتبُّع المتحصلات غير المشروعة وتأمينها واستردادها في آخر المطاف. وقد يسمح بعض بغال المال أيضًا باستخدام حساباتهم في مدةً مخصوصة ومحدودة فقط. وهذه المدة المحدودة، مقرونةً بإجراءات الإعداد المشروعة، تُصعّب نسبيًا على المؤسسات كشف الأنشطة غير الطبيعية.

المربع 11: شركات صورية وحسابات مصرفية وأصول افتراضية

قُدّمت شكاوى متعددة إلى شرطة الهند بشأن استخدام تطبيق للهاتف المحمول للاحتيال على الناس تحت ستار منصة استثمارية لتعدين العملات الرقمية. ووعد التطبيق المستثمرين بحصة من الأرباح المكتسبة من هذا الاستثمار. فقامت الشركة بإغراء الضحايا للاستثمار بشكل أكبر في مخططها وبعد ذلك أوقفت عمليات السحب والدفع. وأصبح الموقع والتطبيق غير قابلين للوصول إليهما، وتوقف القائمون على التطبيق عن إجابة المستثمرين. وطلبت كثير من وكالات إنفاذ القانون التي تتابع التحقيقات في الشكاوى المقدمة من العملاء في أنحاء مختلفة من البلاد الحصولَ على معلوماتٍ من وحدة الاستخبارات المالية الهندية في هذه القضية. وقد حددّ التحليل الذي أجرته وحدة الاستخبارات المالية الهندية كيانين يشغّلان التطبيق على متجر غوغل (Google Play)، وقد حُذِف هذا التطبيق لاحقًا من متجر غوغل. ثم حُدّد 34 كيانًا آخر لارتباطها بهذين الكيانين. ومن بين الكيانات الـ36، كان لدى 28 كيانًا مواطنون أجانب يعملون كمديرين.

ثم بدأت مديرية إنفاذ القانون في الهند أيضًا تحقيقات موازية في جرائم غسل الأموال، كشفت عن مؤامرة إجرامية واسعة النطاق وتورُّط كثير من الكيانات الوهمية في تشغيل تطبيقات أو مواقع احتيالية متشابهة لخداع السذّج واختلاس متحصلات الجريمة. وعند التحقُّق العيني، لم يُعثَر على الكيانات في العنوان المسجل. وبيّن اقتفاء الأثر المالي أنّ العديد من هذه الكيانات متورّطة في تشغيل تطبيقات غير قانونية للمراهنة والقروض، وأنها كانت تغشّ الناس تحت ستار هذه التطبيقات أيضًا. ونُقِلت الأموال غير المشروعة التي جُمِعت من الضحايا إلى حسابات كيانات صورية مختلفة، كما حُوّلَ جزء من متحصلات الجريمة في آخر الأمر إلى أصول افتراضية. وعُثِر على متحصلات الجريمة في هيئة أرصدةٍ متاحة في الحسابات المصرفية التي تحتفظ بها كيانات وهمية مختلفة، قيمتها 865 مليون روبية هندية (أي نحو 9.9 مليون يورو) وتم تجميدها.

المصدر: الهند

30. أبلغت الولايات القضائية أيضًا عن استخدام أنواع أخرى من تقنيات غسل الأموال، بهدف التعتيم على العلاقة بين مختلف الجماعات الإجرامية للاحتيال الذي يسهّل الإنترنت ارتكابه ولغسل الأموال.

- **النقد:** في هذا التقرير دراسات حالات متعددة أوردت أن سحب الأموال النقدية كان عن طريق بغال المال وعصابات الاحتيال الذي يسهّل الإنترنت ارتكابه، وأنه قد يصعب تتبُّع حركة النقد خارج المؤسسات المالية. إذ يمكن سحب الأموال النقدية بأجهزة الصراف الآلي بعد غسلها عبر شبكة لغسل الأموال، وهذا يسمح للمجرمين بتجنب الاتصال وجهًا لوجه بالمؤسسات المالية. وقد تُنقَل هذه الأموال عبر الحدود بواسطة حاملي الأموال النقدية ثم تودع ليتم غسلها أكثر. ويمكن أيضًا استخدام المتحصلات الإجرامية لشراء أشياء ثمينة وأدوات يمكن إعادة بيعها لاحقًا نقدًا، مثل البطاقات السابقة الدفع أو المعادن الثمينة.

13 النقود الإلكترونية هي تمثيل رقمي للعملة الورقية، تستخدم لتحويل القيمة المُقوَّمة بالعملة الورقية تحويلاً إلكترونيًا. النقود الإلكترونية هي آلية تحويل رقمية للعملة الورقية، أي أنها تنقل إلكترونيًا القيمة التي لها صفة العملة الرسمية. مجموعة العمل المالي (يونيو/حزيران 2014) العملات الافتراضية: التعريفات الرئيسية والمخاطر المحتملة في مكافحة غسل الأموال وتمويل الإرهاب

المربع 12: سحب النقود وشراء الذهب وبطاقات الوقود

في مارس/آذار سنة 2023، وقع محاسبٌ في شركة صينية فريسةً لعملية احتيال بانتحال شخصية موظف بنك. إذ تمت إضافته إلى مجموعة على تطبيق المراسلة بدعوى أنه يجب إجراء فحص سنوي لحساب الشركة.

فانتحل المجرمون في مجموعة المراسلة لاحقًا شخصية الممثلين القانونيين للشركة والمساهمين وطلبوا من الضحية تحويل 7.8 مليون يوان صيني (أي نحو 996,000 يورو) إلى حسابَيْن محدَّدين للشركة تحت سيطرة الجماعة الإجرامية. ثم أظهرت تحقيقات الشرطة أن الأموال تم تحويلها إلى 26 حسابًا مصرفيًا ثانويًا، ثم سُحِبَت نقدًا من شباك البنك أو بأجهزة الصراف الآلي، وحُوِّلت إلى منصاتِ دفع تابعة لجهات خارجية، وكذلك استخدمت لشراء الذهب وبطاقات الوقود.

المصدر: الصين

- **غسل الأموال القائم على التجارة أو الخدمات:** هناك كثيرٌ من تقنيات غسل الأموال القائمة على التجارة أو الخدمات التي قد يستخدمها المجرمون لنقل متحصلات الجريمة عبر الحدود.[14] فأما متحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه، فقد لاحظت بعض الولايات القضائية أن المجرمين يستخدمون تقنيات غسيل الأموال القائمة على التجارة، مثل الفواتير الوهمية أو الكاذبة، إضافةً إلى استخدام المتحصلات غير المشروعة لشراء سلع ذات قيمة عالية أو قابلة للتسويق بسهولة (مثل قطع غيار المركبات، والتذاكر، والأدوات المنزلية ...إلخ). ومثال ذلك أنّ بعض الولايات القضائية أبلغت عن تحويلات مصرفية احتيالية إلى شركات مشروعة، تتراوح من علامات تجارية فاخرة أو علامات إلكترونية معروفة إلى شركات محلية صغيرة، وذلك لشراء السلع. إذ يمكن نقل هذه السلع عبر الحدود وتحويلها مرة أخرى إلى أموال نقدية لمزيد من التمويه والإدماج. على أنّ الشركات التجارية التي هي خارج نظام مكافحة غسل الأموال وتمويل الإرهاب قد لا يكون لها الدراية أو المعرفة الكافية لإجراء التحقُّق من الهوية أو مراقبة المعاملات، فيتم استغلالها عن غير قصد من قبل المجرمين. ومن التقنيات التي قد يستخدمها المجرمون في غسل المال أيضًا تقديم فواتير باهظة الثمن أو وهمية لخدمات تكنولوجيا المعلومات أو الخدمات الاستشارية.

14 انظر أيضًا مجموعة العمل المالي ومجموعة إيغمونت (ديسمبر/كانون الأول 2020) غسل الأموال القائم على التجارة: الاتجاهات والتطورات، ومجموعة العمل المالي (يوليو/تموز 2018) غسل الأموال المحترف

المربع 13: الاحتيال الذي يسهّل الإنترنت ارتكابه وبغال المال وغسل الأموال القائم على التجارة

اعتقلت السلطات الأيرلندية شخصًا بارزًا، وهو الشخص (م س)، في مخططٍ لغسل متحصلات الاحتيال بعلاقة غرامية والاحتيال باختراق البريد الإلكتروني التجاري من أيرلندا إلى نيجيريا باستخدام غسل الأموال القائم على التجارة. والتحقيقات ما تزال مستمرة. وإلى الآن، تعتقد السلطات أن مخطط غسل الأموال يشمل ما لا يقل عن 60 اسمًا و64 حسابًا مصرفيًا.

وفي هذا المخطط، حُوّلت متحصلات هذا الاحتيال أولاً إلى الحسابات المصرفية لبغال المال الأيرلنديين. وبعد ذلك سُحِبت الأموال نقدًا وحُوّلت إلى حسابات أيرلندية مرتبطة مباشرة أو مملوكة لشركة الشخص (م س). وقد تبيّن أن كثيرًا من الحسابات المرتبطة بالشخص (م س) مفتوحةٌ بهويات مزورة.

وهناك شركة نيجيرية (يتحكم فيها نيجيريٌّ يعتقد أنّ مقره في الولايات المتحدة) تطلب بضائع من شركات أوروبية أو صينية مشروعة. وهذه الشركات الشرعية تشتغل بالسلع التي يمكن شراؤها وشحنها لإعادة بيعها، ومنها الكحول والملابس والإلكترونيات والأدوية. وبعد ذلك سدّدت الحسابات الأيرلندية الخاصة بالشخص (م س) فواتير الشركة النيجيرية، ثم شحنت البضائع في آخر المطاف إلى الشركة المتواطئة في نيجيريا.

وفي إحدى الوقائع، تلقت شركة أدوية ألمانية أموالاً تزيد على 1.7 مليون يورو لدفع ثمن البضائع التي اشترتها الشركة النيجيرية. فتم اقتفاء أثر هذه الأموال فتبيّن أن لها صلة مباشرة بمتحصلات الاحتيال بعلاقة غرامية والاحتيال باختراق البريد الإلكتروني التجاري عبر أوروبا والولايات المتحدة، وأنها جاءت من حسابات مختلفة، إما مرتبطة بالشخص (م س) أو مملوكة من قِبَله، أو آتية من الضحايا مباشرةً. وقد شُحِنت هذه البضائع في آخر المطاف إلى نيجيريا.

المصدر: إيرلندا

- **جهات تحويل الأموال ومزوّدات خدمات الأصول الافتراضية غير المرخّصة أو غير المسجلة:** قد تُنقَل المتحصلات الإجرامية خارج نطاق الولاية القضائية باستخدام شركات سرية لتحويل الأموال أو خدمات الحوالة مع وجود ضوابط قليلة في حالات لمكافحة غسل الأموال وتمويل الإرهاب أو انعدامها في حالات أخرى. فحيثما تكون الأصول الافتراضية قد تستغل العصابات مزودي خدمات الأصول الافتراضية الموجودين في ولايات قضائية ليس فيها ضوابط لمكافحة غسل الأموال وتمويل الإرهاب أو أن فيها ضوابط ضعيفة.
- **تقنيات تعزيز عدم كشف هوية الأصول الافتراضية:**[15] تُعدُّ المَحافِظ غير المستضافة، والمعاملات التي من نظير إلى نظير، وسلاسل التقشير، ومنصات التداول الشديدة الخطورة، طرقًا مفضّلةً لغسل متحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه ذات الصلة بالأصول الافتراضية بسرعةٍ خارج نطاق الولاية القضائية، وغالبًا ما يتم استخدامها مجتمعةً. ويتزايد أيضًا استخدام المجرمين لأجهزة الصراف الآلي الخاصة بالبيتكوين لتحويل القيمة وطمس هوية الذين يتحكمون في الأموال، ومثال ذلك أنهم يقدّمون وثائق هوية مزورة أو معدلة مثل المُعرّفات المختلفة أو أرقام هواتف مختلفة أو تواريخ ميلاد مختلفة عند إيداع الأموال أو سحبها. كما أنهم يستخدمون أيضًا تقنيات التعتيم، ومن ذلك استخدام خدمات الخلط والتقليب، إضافةً إلى استخدام أصول افتراضية معزّزة لإخفاء الهوية (وتسمى أيضًا عملات الخصوصية، كعملة مونيرو Monero) وخدمات التمويل غير المركزي (DeFi).

15 بُحِثت هذه التقنيات باستفاضة في تقرير مجموعة العمل المالي (مارس/آذار 2023) مكافحة تمويل برمجيّات انتزاع الفدية

المربع 14: غسل الأموال المعقّد في قطاعات متعددة

استهدفت عصابة أجنبية للاحتيال بعلاقات غرامية ما يقرب من 70 ضحية يابانية. وحُوّلت أموالٌ بقيمة 3 ملايين دولار أمريكي إلى حسابات مصرفية مختلفة لبغال المال في اليابان. فقام رجل ياباني، وهو الراعي المحلي لبغال المال، بغسل الأموال وإرسالها إلى غانا، حيث كان مقر عصابة الاحتيال. وفي آخر المطاف، اعتُقل الرجل الياباني بالتعاون مع غانا عبر الإنتربول.

وبعد ذلك حُوّلت الأموال من حسابات بغال المال إلى حساب راعيهم الياباني. وتبيّن في تحليل ورد في تقرير المعاملات المشبوهة أن الأموال غُسِلت من خلال ثلاث قنوات من قبل راعي بغال المال الياباني:

- أُجريت تحويلات برقية إلى حساب مصرفي يملكه راع ياباني لبغال المال في غانا. ثم سُحِبت الأموال نقدًا في غانا وسُلِّمت باليد إلى زعيم العصابة الذي ما يزال طليقًا. وفي أثناء إجراء التحويلات البرقية، قدم الرجل الياباني فواتير وهمية إلى البنك الياباني الذي يتعامل معه، وأعلن زورًا أنها لنشاط تجاري مشروع (شراء حبوب الكاكاو).
- وقد حُوّلت بعض الأموال إلى أصول افتراضية من خلال مزوّد لخدمات الأصول الافتراضية في اليابان.
- وحُوّلت الأموال أيضًا إلى غانا من خلال بنك سري مرتبط بالجالية الغانية في اليابان.

المصدر: اليابان

تأثير الرقمنة والتقنيات الجديدة على غسل الأموال

31. أتت التكنولوجيات الجديدة بفوائد وفرص جديدة للمستهلكين. وهناك تحول عميق نحو رقمنة الخدمات المالية، وقد تسارع هذا التحوُّل خلال جائحة كوفيد-19. إذ أدى انخفاض استخدام النقد وزيادة النشاط عبر الإنترنت إلى ظهور أدوات وعمليات جديدة ومبتكرة. كما أن سلسلة الدفعات المالية تنمو بشكل متزايد نموًّا ديناميكيًّا ومجزّأً، مع زيادة التنوع في مزوّدات الخدمات التي يتقدّم خدمات الدفع والمعاملات (انظر أيضًا القسم 3-1 أدناه).

32. هذا من جهة، ولكن من جهة أخرى يمكن أن يكون التطوّر التكنولوجي مفيدًا للجماعات الإجرامية التي تستغل هذه الفرص لتحسين تقنياتها في غسل الأموال تحسينًا كبيرًا. إذ إنّ المعاملات المالية تُنفَّذ بشكل متزايد بسرعات شبه فورية، ومن أسباب ذلك توقعات المستهلكين بأن ينفذوا معاملاتهم من غير بذل جهد. وكما ذكرنا سابقًا، فإنه إذ قُرن كل ذلك بتقنيات إخفاء الهوية الرقمية مثل الشبكات الخاصة الافتراضية، صار من الصعب على السلطات تحديد المجرمين النهائيين الذين يقومون بمعاملات غسل الأموال بتتابع سريع.

33. أفضت الرقمنة إلى زيادة سهولة إنشاء الحسابات وسرعتها بغرض غسل الأموال وتوسّع عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه عبر الحدود. ولاحظت بعض الولايات القضائية ارتفاعًا في العمليات الافتراضية عن بُعد في مجالَين: فتح الحسابات وإنشاء الشركات. ومثل هذه العمليات الافتراضية عن بُعد تلغي الحاجة إلى السفر الفعلي. فيمكن للمجرمين حينئذٍ استغلال هذه الفرص ليغسلوا الأموال.

المربع 15: التوسُّع من خلال الرقمنة

توصّل تحليلٌ لوحدة استخبارات مالية إلى شبكة واسعة تتكون من 147 فردًا و276 حسابًا مصرفيًا من ثمانية بنوك. قد تخلى هؤلاء الأفراد عن هويتهم الرقمية الوطنية المخصصة لتحديد هوية المستخدم على منصة الحكومة وغيرها من المنصات عبر الإنترنت، وأعطوها لعصابات إجرامية. ثم استخدمت العصابات الهوية الرقمية لفتح حسابات مصرفية عن بُعد فسيطروا سيطرةً مباشرة على هذه الحسابات ليغسلوا متحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه. وكشفت وحدة الاستخبارات المالية الشبكة بتحديد القواسم المشتركة كالمعاملات المصرفية المشتركة ونقاط البيانات المشتركة (أي معلومات الاتصال الأجنبية ومعرّف الجهاز)، إضافةً إلى تفاصيل الاتصال (أي البريد والبريد الإلكتروني والهاتف).

فأُحيلت المعلومات الاستخبارية إلى قيادة مكافحة الاحتيال (ASCom)، وهي الوحدة السنغافورية المختصّة بمكافحة الاحتيال الذي يسهّل الإنترنت ارتكابه وما يتصل به من غسل الأموال، وهي تابعة لشرطة سنغافورة. وأدت تحقيقات قيادة مكافحة الاحتيال في النهاية إلى القبض على 6 من الرعايا ومحاكمة 3 أفراد لاشتراكهم في المخطط الإجرامي.

المصدر: سنغافورة

34. يمكن أن يوسّع المجرمون حجم شبكة بغال المال سريعًا (وهي عابرة للحدود الوطنية في كثير من الأحيان)، وذلك بالاستفادة من أدواتٍ رقمية يوسّعون بها نطاق تعيين بغال المال عبر الحدود واستخدامهم. وقد تم أيضًا تحديد تطبيقات لنقل الصوت على بروتوكول الإنترنت (VoIP) وتبيّن أنها الوسائط المفضّلة في عملية التعيين. ودرجت العادة بأن يكون هناك قدرٌ من الخلاف في عمليات غسل الأموال بين شبكات بغال المال، فإن تلقي بغال المال للتعليمات من العصابات الإجرامية الأخرى والامتثال لها محتاج إلى وقت. فتم تقصير هذه المدد الزمنية كثيرًا بعد أن صارت عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه تستخدم منصات المراسلة الفورية.

35. قد يقوم المجرمون بسرقة الهويات على نحو متزايد بتقنياتٍ وأدوات تكنولوجية شتّى، ومنها التصيُّد الاحتيالي أو الشراء أو خداع شخص ما لتسليم هويته طوعًا. وفي بعض الأحيان، قد يستخدمون هويات مزورة وهويات اصطناعية، يجمعون فيها مزيجًا من معلومات الهوية الحقيقية والمزيفة لإنشاء حسابات احتيالية. ثم يقوم المجرمون مباشرةً بإعداد حسابات والتحكم فيها باستخدام هذه الهويات المسروقة أو المزورة. وهذا إنما يزيد من صعوبة تتبُّع أنشطة غسل الأموال، لأن أصحاب الحسابات قد لا يكونون على علمٍ بإشراكهم.

36. أشار أحد الوفود إلى المخاطر المحتملة في استخدام تركيب الصور المزيفة (deepfake) في عمليات الاحتيال للاستيلاء على الحسابات. فبمساعدة خوارزميات تعلم الآلة، قد يركّب المحتال صوتًا مزيفًا لأحدٍ أو مقطع فيديو له، وهو ما يمكن استخدامه بعد ذلك لانتحال شخصية ذلك الشخص عبر الهاتف أو في أنظمة الاستيقان بالاستدلال الحيوي (biometric). وقد تُستخدَم أيضًا تقنيات تركيب الصور المزيفة مع تقنيات الهندسة الاجتماعية لخداع الضحايا حتى يعطوا بيانات تسجيل دخولهم إلى حساباتهم. لكن ما تزال تقنية تركيب الصور المزيفة جديدةً نسبيًا، وهذا يعني أن خطر عمليات الاحتيال للاستيلاء على الحساب المعتمدة على تركيب الصور المزيفة قد يكون محدودًا إلى حدٍّ ما في الوقت الحالي. على أنه قد يشكل خطرًا كبيرًا في المستقبل إذا استمر تطوّر هذه التكنولوجيا وأصبحت متاحة في نطاق أوسع.

المربع 16: سرقة الهوية عن بُعد للتحكم المباشر

في سلسلة من عمليات الاحتيال المتعلقة بالتصيُّد، خدع المجرمون ضحاياهم فاستطاعوا أن يثبّتوا أدوات الوصول عن بُعد في أجهزة الحاسوب الخاصة بالضحايا. وفي العديد من الحالات، أنشؤوا حسابات باستخدام مزوّدات خدمات الأصول الافتراضية باسم الضحية دون علمها. واستطاع المجرمون فعل ذلك باستخدام البيانات التي سرقوها بأدوات الوصول عن بُعد. ويُشتبَه أيضًا بأن المجرمين قاموا بتوجيه الضحايا خلال عملية فتح حساب التحقّق عبر الإنترنت، واستخدموا لإتمام ذلك أدوات الوصول عن بُعد فأخفوا الواجهات الفعلية.

فخُدِع الضحايا أخيرًا وحوّلوا الأموال إلى حسابات مفتوحة في مزوّدات خدمات الأصول الافتراضية المذكورة. وتمكن المجرمون من استخدام هذه الحسابات مباشرةً في علميات غسل الأموال التي شرعوا بها لاحقًا. وتشير التقديرات إلى أن مُجمَل ما فقده الضحايا هو أكثر من 600,000 يورو في هذه السلسلة من الاحتيالات.

المصدر: النمسا

3 أوجه الضعف الأخرى الناشئة في غسل الأموال

37. توفر التدابير الوقائية المطلوبة للمؤسسات المالية والأعمال والمهن غير المالية المحددة ومزوّدي خدمات الأصول الافتراضية بموجب معايير مجموعة العمل المالي (في التوصيات من 9 إلى 23) أساسًا لمنع دخول متحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه إلى القطاع المالي وغيره من القطاعات. ويركّز هذا القسم على أوجه الضعف الناشئة في غسل الأموال، وهي أوجه يمكن أن تستغلّها عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه.

3-1 المخاطر الناشئة عن المؤسسات المالية الرقمية[16]

38. أدّى تطور أساليب الدفعات المالية إلى ظهور مؤسسات مالية رقمية جديدة، مثل مزوّدي خدمات الدفع (PSP)، وإصدار النقود الإلكترونية ...إلخ. على أنه يمكن أن يكون لدى المؤسسات المالية التقليدية مزيدٌ من الموارد تحت تصرُّفها، وهذا قد يؤدي إلى ضوابط أقوى نسبيًا من ضوابط هذه المؤسسات المالية الرقمية الأحدث. وربما أدّى ذلك إلى انزياحٍ، فيسعى المجرمون إلى استغلال أوجه الضعف لدى مزوّدي الخدمات المالية البديلين لغسل الأموال.

39. يمكن أيضًا أن تكون شبكة الدفعات مجزّأةً. فتكون هناك علاقات مالية متداخلة مختلفة بين هذه المؤسسات، وذلك مثل العلاقة بين مؤسسات الدفع المختلفة التي تتعامل بعضها مع بعض أو تقدّم حسابات لمزوّدي الخدمات التي هي أصغر، فتقدّم هذه الخدمات الصغرى بدورها أنواعًا أخرى من الخدمات المالية (انظر أيضًا المربع 17 أدناه). ومن الممكن أن تفضي هذه التجزئة أيضًا إلى تفاقم الصعوبات في تتبُّع المعاملات عبر أنواع مختلفة من المؤسسات الداخلة في "سلسلة الدفع". وربما أنشأ هذا أيضًا تحديات في ضمان التوافر الفوري للمعلومات الأساسية عن مُنشِئ التحويلات والمستفيد منها عبر سلسلة الدفع[17].

40. ينبغي تمشيًّا مع معايير مجموعة العمل المالي أن يكون هناك إشراف تنظيمي قوي على المؤسسات المالية الجديدة، ومن ذلك الإشراف على الترخيص أو التسجيل المناسبَين، ومنع المجرمين أو شركائهم من السيطرة على هذه الكيانات. وينبغي للسلطات التنظيمية التأكد من أن لدى جميع المؤسسات التي تجري المعاملات رقابةً كافيةً على محيطها، فكل المؤسسات تتحمل مسؤولية إجراء أو العناية الواجبة تجاه العملاء أو ضمان إجرائها ورصد المعاملات على عُقَد المرسلين والمستفيدين.

المربع 17: إساءة استخدام قطاع مزوّدي خدمة الدفع

حدّد التحليل الذي أجرته هيئة الرقابة الفرنسية في النصف الأول من عام 2021 مزوّدات خدمات الدفع الرئيسية التي تُستخدَم لتلقّي التحويلات المصرفية الاحتيالية. فتبيّن أن مزوّدات خدمات الدفع الرئيسية هذه عادةً ما تقدّم "الخدمات المصرفية كخدمة"، مع وجود فرع لبعضها في فرنسا لغرض وحيد، ألا وهو تقديم أرقام فرنسية للحسابات المصرفية الدولية (IBAN)، مع الحد الأدنى من الوجود المادي.

ووجد التحليل أن مزوّدات خدمات الدفع الرئيسية كانت أكثر خطورةً بنحو 200 مرة من المؤسسات الأخرى. فقد كان في معظم مزوّدات خدمات الدفع هذه ضعف في التحقّق من الهوية ورصد المعاملات. إذ فتح المجرمون حسابات بهويات أساؤوا استخدامها فأمكنهم التحقق بسرعة مما إذا كانت بعض الحسابات المفتوحة قد حُدِّدت على أنها احتيالية بواسطة مزود خدمة الدفع أم لا، وذلك من خلال محاولتهم تنفيذ معاملات بمبالغ زهيدة أولاً وتغيير وجهة الأموال إذا لزم الأمر. وبعد ذلك حوَّلوا الأموال المكتسبة بالاحتيال بسرعةٍ إلى حساب واحد أو عدّة حسابات. وتقسيم المبالغ بين عدة حسابات يؤدّي إلى تمكين المجرمين من التحايل على القيود التي يفرضها مزود خدمة الدفع في خدماته، مثل حدود السحب النقدي أو البقاء تحت عتبة رصد العمليات التي يحدّدها مزود خدمة الدفع داخليًا.

المصدر: فرنسا

16 يقرّ هذا التقرير أيضًا بمخاطر غسل الأموال الناشئة عن الأصول الافتراضية ومزوّدي خدمات الأصول الافتراضية. ولمزيد من المعلومات حول المخاطر والتحديات التنظيمية المتعلقة بمزوّدي خدمات الأصول الافتراضية، انظر رجاءً مجموعة العمل المالي (مارس/آذار 2023) مكافحة تمويل برمجيّات انتزاع الفدية، وانظر أيضًا (يونيو/حزيران 2023) تحديث مستهدف حول تنفيذ معايير مجموعة العمل المالي للأصول الافتراضية ومزودي خدمات الأصول الافتراضية.

17 تنظر مجموعة العمل المالي أيضًا في ما يمكن إدخاله من التعديلات على التوصية ذات الرقم 16 (بشأن التحويلات البرقية) لمراعاة التطورات الأخيرة والمقبلة في بنية أنظمة الدفع.

2-3 إساءة استخدام رقم الحساب المصرفي الدولي الافتراضي[18]

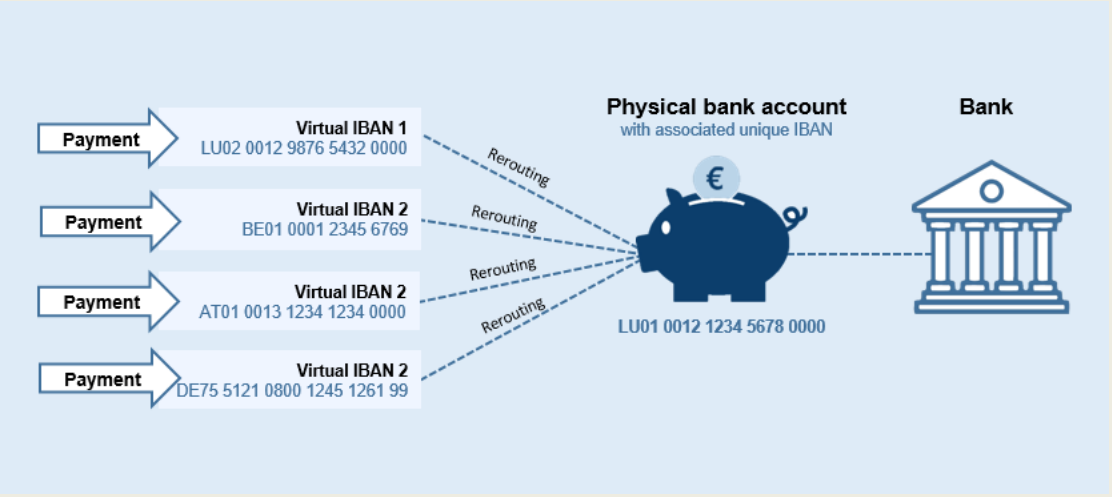
41. هنا مثال آخر لكيفية استغلال الابتكار المالي لأغراض الاحتيال الذي يسهّل الإنترنت ارتكابه، وهو استخدام أرقام الحسابات المصرفية الدولية الافتراضية (vIBAN). فهناك كثير من المؤسّسات التي تصدر هذه الأرقام للعملاء، ومنها البنوك ومزوّدي خدمات الدفع. وصحيح أنّ أرقام الحسابات المصرفية الدولية الافتراضية تُستخدَم بعدة طرق مشروعة مختلفة، كتيسير وتصنيف الدفعات من أطراف متعدّدة، ولكن أبلغ كثير من الولايات القضائية عن إساءة استخدام أرقام الحسابات المصرفية الدولية الافتراضية وتصييرها أداةً لغسل الأموال المتصلة بالاحتيال الذي يسهّل الإنترنت ارتكابه.

المربع 18: ما هو رقم الحساب المصرفي الدولي الافتراضي؟

إنّ رقم الحساب المصرفي الدولي الافتراضي مطابقٌ من الوجهة الوظيفية لرقم الحساب المصرفي الدولي التقليدي، إذ يمكن استخدامهما لإرسال واستقبال الدفعات على نطاق عالمي. حتى إنه يبدو مثل نظيره التقليدي ويتكون أيضًا ممّا يصل إلى 34 حرفًا أبجديًا رقميًا. فمن الناحية الوظيفية والمرئية، لا يمكن تمييزه عن رقم الحساب المصرفي الدولي المألوف.

يكمن الاختلاف الرئيسي بين رقمي الحساب المصرفي الدولي المألوف والافتراضي في مطابقة الحساب. فرقم الحساب المصرفي الدولي المألوف مطابق بنسبة 1:1 مع الحساب المصرفي، وهذا يعني أنه لا يوجد سوى حساب مصرفي فعلي واحد مرتبط بكل رقم حساب مصرفي دولي واحد. لذلك، إذا استخدم شخص ما رقم الحساب المصرفي الدولي لإجراء دفعةٍ به، فسوف تنتهي الأموال تلقائيًا إلى الحساب المصرفي الذي يرتبط به ذلك الرقم.

وعلى النقيض من ذلك، فإن رقم الحساب المصرفي الدولي الافتراضي هو رقم افتراضي لا يتطابق مع حساب في بنك فعلي. فهي عبارة عن أرقام مرجعية يصدرها البنك تتيح إعادة توجيه الدفعات الواردة على رقم الحساب المصرفي الدولي الحقيقي الذي هو في حد ذاته مرتبط بحساب مصرفي فعلي. فلا يمكن أن تحفظَ أيّ أموال، ورصيدها صفر دائمًا. ويمكن لممتلكي رقم الحساب المصرفي الدولي الافتراضي الحصول أيضًا على كثير من أرقام الحسابات المصرفية الدولية الافتراضية الفريدة، وهذه الأرقام تُعِيد توجيه جميع الدفعات وتمركزها في حساب مصرفي فعلي واحد، كما هو موضح في الشكل 3.

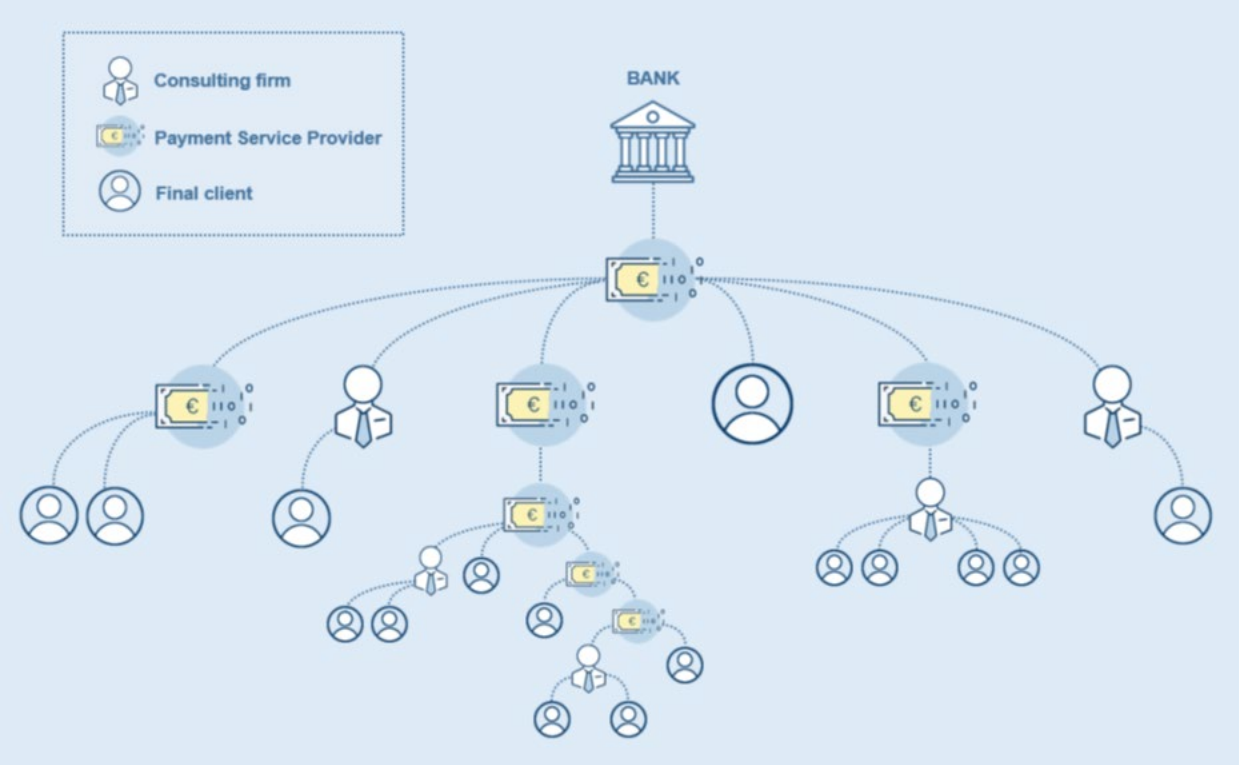


المصدر: شراكة اليوروبول بين القطاعين العام والخاص في الاستخبارات المالية

18 لمزيد من المعلومات حول المخاطر والتحديات المرتبطة أرقام الحسابات المصرفية الدولية الافتراضية، انظر: (يونيو/حزيران 2023) شراكة اليوروبول بين القطاعين العام والخاص في الاستخبارات المالية (EFIPPP) معلومات استخباراتية للتهديدات الواقعة على أرقام الحسابات المصرفية الدولية الافتراضية (لا يُتاح إلا لأعضاء شراكة اليوروبول للاستخبارات المالية بين القطاعين العام والخاص).

42. ونظرًا إلى أن أرقام الحسابات المصرفية الدولية المألوفة وأرقام الحسابات المصرفية الدولية الافتراضية متطابقةٌ بصريًّا، فإن المجرمين يستخدمونها في خداع الضحايا فيجعلونهم يعتقدون أنهم يحوّلون الأموال إلى حساب مصرفي، في حين أنه بدلاً من ذلك يمكن أن يكون الرقم الذي أرسلوا إليه هو رقم حساب مصرفي دولي افتراضي مثلاً يستخدم لغرض إضافة رصيد إلى محفظة إلكترونية. ولزيادة تعقيد الأمور، يمكن إعادة إصدار أرقام الحسابات المصرفية الدولية الافتراضية من قبل عميل مؤسسة مالية، ولا سيّما إذا كان العميل مؤسسة مالية أخرى. وهذا إنما يصعّب تحديد البلد الأصلي لرقم الحساب المصرفي الدولي الافتراضي وموقع الحساب الرئيسي.

الشكل 2: شبكة تُظهِر توالِيَ إصدار رقم حساب مصرفي دولي افتراضي وإعادة إصدار أرقام الحسابات المصرفية الدولية الافتراضية



المصدر: شراكة اليوروبول بين القطاعين العام والخاص في الاستخبارات المالية

43. وخلاصة القول أنه يمكن للمجرمين إساءة استخدام أرقام الحسابات المصرفية الدولية الافتراضية لإخفاء معلومات المستفيد النهائي وسَتر حركة الأموال غير المشروعة. وهذا يصعّب تحديد مكان الحساب الرئيسي الحقيقي والمؤسسة المالية المُصْدِرة، وكذلك يصعّب ضمان رصد المعاملات رصدًا صحيحًا. وفي آخر المطاف يؤدي هذا إلى تحديات تواجهها السلطات المختصة لتحديد الحسابات المادية وتجميد الأموال (لأن أرقام الحسابات المصرفية الدولية الافتراضية هي مجرّد أرقام مرجعية صادرة عن البنك وليست حسابات حقيقية تحوي أرصدةً مادية). ومما يعدّ ممارسةً جيّدة أن بعض الولايات القضائية عملت مع البنوك التي تصدر أرقام الحسابات المصرفية الدولية الافتراضية للتعرُّف بسرعة على مؤسسة الدفع المرتبطة بهذه الحسابات الرئيسية عندما يتم تحديد وقوع الاحتيال الذي يسهّل الإنترنت ارتكابه.

المربع 19: إساءة استخدام أرقام الحسابات المصرفية الدولية الافتراضية لغرض للاحتيال الذي يسهّل الإنترنت ارتكابه

بين شهر فبراير/شباط ومارس/آذار من سنة 2023، تلقّت وحدة الاستخبارات المالية في لوكسمبورغ عدّة تقارير عما يسمى خِدَع "مرحبًا أمّي" (Hi Mum)، إذ ورد على الضحايا رسائل وتساب من رقم هاتف غير معروف ولكنه محلي من محتالين يتظاهرون بأنهم أطفالهم. وتلقى الضحايا رسائل نصية باللغة اللوكسمبورغية، عبر أرقام لوكسمبورغية من هواتف محمولة، مُضمَّنٌ فيها رقم حساب مصرفي دولي لوكسمبورغي.

وفي أثناء التحقيق في هذه القضية، كشفت وحدة الاستخبارات المالية في لوكسمبورغ أن أرقام الحسابات المصرفية الدولية التي أرسلها المحتالون كانت عبارة عن أرقام حسابات مصرفية دولية افتراضية. وقد صدرت أرقام الحسابات المصرفية الدولية الافتراضية عن مؤسسة مصرفية في لوكسمبورغ وأُعطِيَت لمزوّدٍ لخدمة الدفع في لوكسمبورغ يقدّم بطاقات ائتمان سابقة الدفع للعملاء الأوروبيين. وبطاقات الائتمان السابقة الدفع هذه يمكن إيداع المال فيها عن طريق تحويل الأموال إلى أرقام حسابات مصرفية دولية افتراضية، وهي التي كان المجرمون يعتزمون استخدامها لمزيد من عمليات غسل الأموال.

ومن بين ستّةٍ من أرقام الحسابات المصرفية الدولية الافتراضية التي تبيّن أنها استُخدِمت في عملية الاحتيال، تمكنت وحدة الاستخبارات المالية في لوكسمبورغ من حظر أو استرجاع 40,000 يورو من أصل 55,000 يورو من الأموال المستلبة بالاحتيال. وقد يُسِّر عمل وحدة الاستخبارات المالية في لوكسمبورغ بقيامِ تعاونٍ بين وحدة الاستخبارات المالية والبنك الذي أصدر أرقام الحسابات المصرفية الدولية الافتراضية، وذلك أتاح التعرُّف بسرعةٍ على مؤسسة الدفع التي كان فيها الحساب الأساسي للعميل النهائي.

المصدر: لوكسمبورغ

3-3 القطاعات غير التقليدية

44. سلّطت كثير من الولايات القضائية الضوء على أهمية العمل مع القطاعات غير التقليدية، ومنها منصات وسائل التواصل الاجتماعي، والتجارة الإلكترونية، ومزوّدي خدمات الاتصالات والإنترنت، في مكافحة غسل الأموال المتّصل بالاحتيال الذي يسهّل الإنترنت ارتكابه. ومع أن هذه القطاعات غير التقليدية لا تخضع للتنظيم فيما يتعلق بمكافحة غسل الأموال وتمويل الإرهاب، إلا أن في حوزتها معلومات مفيدة يمكن أن تعين على تعزيز تحقيقات غسل الأموال، ولا سيّما حين تُستخدَم للاحتيال الذي يسهّل الإنترنت ارتكابه وتعيين بغال المال. فإن منصات وسائل التواصل الاجتماعي، وكذلك مزوّدي خدمات الاتصالات والإنترنت، يمكن أن تتيح معلومات جنائية رقمية هامّة جدًّا، ومنها عناوين بروتوكول الإنترنت وأرقام الهواتف وعناوين البريد الإلكتروني وما إلى ذلك، وهذه الأشياء يمكن أن تساعد في تحديد مرتكبي الجرائم الجنائية النهائيين. وحينما تُستخدَم مواقع الإنترنت الاحتيالية أو الإعلانات الاحتيالية للاحتيال الذي يسهّل الإنترنت ارتكابه، فإن في حوزة هذه القطاعات أيضًا معلومات عن المعاملات المالية والدفعات المرتبطة بالمجرمين (ومثال ذلك: تفاصيل الدفع لاستضافة مواقع الإنترنت والإعلانات).

45. أظهرت التجارب ودراسات الحالة من الولايات القضائية أيضًا كيف يمكن إساءة استخدام التجارة الإلكترونية أو وسائل التواصل الاجتماعي أو البثّ المباشر أو منصات الألعاب وتصييرها وسيلةً لغسل متحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه. فإن الاستخدام الواسع النطاق لوسائل التواصل الاجتماعي أو منصات البث أو الألعاب يتيح للمستخدمين تلقّي التبرُّعات أو الهدايا أو الرموز المميزة أو الرصيد من المشاهدين والجمهور. وقد يستغل المجرمون غياب شروط مكافحة غسل الأموال وتمويل الإرهاب ويستخدمون مثل هذه المنصات لغسل متحصلات الجريمة.

المربع 20: متحصلات التصيُّد التي تُغسَل عبر وسائل التواصل الاجتماعي ومنصة البثّ المباشر

اكتُشِف تعرُّض تسعة عشر حسابًا مصرفيًا لخسائر بسبب هجوم تصيُّد استهدف عملاء بعض البنوك. وكشف تحليلٌ أجرته وحدة الاستخبارات المالية الألمانية أن المعاملات من هذه الحسابات المصرفية جرت من خلال حسابات دفع مملوكة لاثنين من المستخدمين. وأنّ هذه الأموال أُرسِلت لاحقًا إلى وسائل التواصل الاجتماعي ومنصة بث مباشر. ثم استخدمت الأموال لإعادة شحن حسابات المستخدمَيْن الموجودة على منصة البثّ بـ"العملة المعدنية" (وهي عملة محلية يتداولها مستخدمو المنصة) التي يمكن استخدامها لشراء هدايا افتراضية. ويمكن تحويل هذه الهدايا إلى مُنشِئي المحتوى الذين يستطيعون تحويل هذه العملات إلى عملة نظامية وسحب القيمة النقدية المكافئة.

والتحقيقات ما تزال مستمرة. وقد أظهرت بيانات عنوان بروتوكول الإنترنت أنه المعاملات الاحتيالية نُفِّذت من نفس عناوين بروتوكول الإنترنت لتسجيل الدخول. ويشير تحليل وحدة الاستخبارات المالية إلى أن أحد المجرمَيْن المشتركين يقوم بغسل أجزاء كبيرة من متحصلات التصيُّد عبر وسائل التواصل الاجتماعي ومنصة البث المباشر من أجل أن يتصرّف بالأموال لاحقًا.

المصدر: ألمانيا

4 الاستجابات والإستراتيجيات التشغيلية الوطنية

46. يناقش هذا الفصل أولاً المصادر الرئيسية للمعلومات التي تعتمد عليها الولايات القضائية للكشف عن الاحتيال الذي يسهّل الإنترنت ارتكابه والتحقيق فيه. ثم يستكشف بنيات التنسيق والتعاون المحلية، وكيف تستفيد الولايات القضائية من هذه البنيات للتحقيق في حالات الاحتيال الذي يسهّل الإنترنت ارتكابه وغسل الأموال المتصل به ومنعهما.

4-1 أهمّ مصادر الكشف

47. بناءً على ما ورد من تجارب الولايات القضائية ودراسات الحالة، فإن هناك مصدرَيْن رئيسيَّيْن للمعلومات لكشف غسل الأموال المتصل بالاحتيال الذي يسهّل الإنترنت ارتكابه والتحقيق فيه، ألا وهما: بلاغ الضحايا وتقارير المعاملات المشبوهة.

48. للولايات القضائية أيضًا مبادراتٌ مختلفة تُعزّز بها عملية الإبلاغ لتحقيق أقصى قدر من تمام المعلومات التي يمكنها الوصول إليها من أجل الإنفاذ الفعّال. فباستخدام هذه المعلومات والبيانات تستفيد السلطات المختصّة من الاستراتيجيات والأدوات الرقمية في تحليل المجموعات الإجرامية وتحديدها من أجل بلوغ إنفاذٍ أكثر فعّاليةً وأدق هدفًا[19].

بلاغ الضحايا

49. يعدُّ بلاغ الضحايا مصدرًا هامًّا للمعلومات لكشف المتحصلات غير المشروعة المتصلة بالاحتيال الذي يسهّل الإنترنت ارتكابه والتحقيق فيها. ففي بعض عمليات الاحتيال مثل الاحتيال باختراق البريد الإلكتروني التجاري والاحتيال بالتصيُّد، عادةً ما يكتشف الضحايا سريعًا أنهم تعرّضوا للاحتيال (ومثال ذلك حين يبدأ الطرف المقابل الصحيح بطلب دفعات لم تصل إليه بعد). وأما في أنواع أخرى من قضايا الاحتيال الذي يسهّل الإنترنت ارتكابه، كالاحتيال بالاستثمار أو الاحتيال بعلاقة غرامية أو بالتصيُّد، فقد لا يدرك الضحايا أنهم تعرّضوا للاحتيال إلا بعد انقضاء بعض الوقت.

50. إن سرعة بلاغ الضحايا أمرٌ مهمٌّ يُمكِّن السلطات المختصة من التصرف عاجلاً لتتبّع المتحصلات غير المشروعة وربما زاد من احتمال نجاح نتائج الإنفاذ. وللضحايا أن يبلّغوا عن الجرائم المشتبه بها إلى وكالات إنفاذ القانون، ومنها الوحدات المتخصصة التي تتعامل مع تقارير الاحتيال. وللضحايا أيضًا إخطار مؤسّساتهم المالية ومزّدي خدمات الدفع ومزوّدي خدمات الأصول الافتراضية بالمعاملات الاحتيالية التي يشتبهون بها في حساباتهم. وأشارت ولايات قضائية أخرى إلى أنه يجوز للضحايا أيضًا اللجوء إلى هيئات الحماية المالية للمستهلك بدلاً من سلطات إنفاذ القانون.

51. لكن من المرجّح أن تبليغ الضحايا عن الاحتيال الذي يسهّل الإنترنت ارتكابه قليل جدًّا، ولا سيّما حين يتكبدون خسارة ضئيلة. فإذا قُرن ذلك بالعوامل العاطفية، ومنها الإحراج أو الخوف، فقد يقرّر الضحايا عدم التقدّم ببلاغ عن ذلك.

52. ومما يعدّ ممارسةً جيّدةً لزيادة بلاغ الضحايا إنشاء بعض الولايات القضائية لمنصاتٍ مخصّصة للضحايا حتى يبلغوا بها عن الاحتيال الذي يسهّل الإنترنت ارتكابه، ومن ذلك إنشاء البوابات الإلكترونية. وتوفّر هذه المنصات تنسيق التقارير على نحوٍ منظّم لتوحيد جمع البيانات، وهذا إنما يُيسِّر التحليل الجمعي لتقارير الضحايا، ويمكن أن يُعينَ على تحديد الاتجاهات والأنماط الإجرامية. وأيضًا يمكن أن تتضمن المنصات موارد مفيدة للوقاية من الاحتيال الذي يسهّل الإنترنت ارتكابه ومساعدة الضحايا.

19 لمزيد من المعلومات التي توضح كيف يمكن لوحدات الاستخبارات المالية ووكالات إنفاذ القانون الاستفادة من التحوُّل الرقمي لتبلغ إلى تحليلٍ وتحقيقٍ فعّالَيْن في مكافحة غسل الأموال وتمويل الإرهاب، انظر التقارير السرية حول التحوُّل الرقمي لمكافحة غسل الأموال وتمويل الإرهاب للسلطات التشغيلية: مجموعة إيغمونت-مجموعة العمل المالي (أكتوبر/تشرين الأول 2021) كشف الأنشطة المشبوهة وتحليل الاستخبارات المالية (المرحلة الأولى)، ومجموعة العمل المالي (مايو/أيار 2022) سلطات إنفاذ القانون وتبادل المعلومات (المرحلة الثانية).

المربع 21: مركز مكافحة الاحتيال في المملكة المتحدة

إن مركز مكافحة الاحتيال (Action Fraud) هو المركز الوطني للإبلاغ عن الاحتيال والجرائم الإلكترونية في المملكة المتحدة. وهو يتيح نقطة اتِّصال مركزية لمكافحة الاحتيال وجرائم الإنترنت ذات الدوافع المالية، وتديره شرطة مدينة لندن مع المكتب الوطني المعني باستخبارات الاحتيال (NFIB). وفي موقع Action Fraud كثيرٌ من موارد التوعية العامّة للوقاية من الجريمة إضافةً إلى حماية الضحايا ودعمهم.

ويتيح موقع Action Fraud أيضًا للضحايا بوابةً للإبلاغ المباشر عبر الإنترنت على مدار الساعة طوال أيام الأسبوع. وتُنقَل البلاغات التي في الموقع إلى المكتب الوطني المعني باستخبارات الاحتيال فيقدّرها ويحلّلها عبر أجزاء مختلفة من البلاد لتحديد الجناة النهائيين. وبعد ذلك تُرسَل هذه البلاغات إلى الشرطة المحلية المناسبة داخل المملكة المتحدة لإجراء التحقيقات. ويستخدم المكتب الوطني المعني باستخبارات الاحتيال أيضًا هذه البلاغات لمصادرة الحسابات المصرفية والمواقع الإلكترونية وأرقام الهواتف التي يستخدمها المحتالون.

المصدر: المملكة المتحدة

تقارير المعاملات المشبوهة

53. لمّا كان احتمال أن يكون بلاغ الضحايا قليلاً جدًّا، صارت تقارير المعاملات المشبوهة مصدرًا مستقلاً شديد الأهمية للكشف عن التدفقات المالية المتصلة بالاحتيال الذي يسهّل الإنترنت ارتكابه.

54. وجاء في البيانات التي جمعتها وحدات الاستخبارات المالية أنّ تقديم معظم تقارير المعاملات المشبوهة المتعلقة بالاحتيال الذي يسهّل الإنترنت ارتكابه قدَّمَها القطاع المصرفي. ومع ذلك، يجب على البنوك أن تستمر في تعزيز قدراتها على كشف الاحتيال الذي يسهّل الإنترنت ارتكابه وغسل الأموال المتصلة به، إذ إنّ عصاباته لا تنفكّ تُطوِّر طريقة عملها. وكشفت البيانات أيضًا أن خدمات تحويل القيمة المالية (MVTS) ومزوّدي خدمات الأصول الافتراضية قدّمت عددًا أقلّ من تقارير المعاملات المشبوهة بالقياس إلى غيرها من المؤسسات. وقد يكون السبب في ذلك أن قطاع خدمات الأصول الافتراضية في بعض الولايات القضائية غير منظّم بالكُلّيّة بما يتمشّى مع معايير مجموعة العمل المالي.[20]

55. ومن المهم ضمان إجراء تحليل سريع لتقارير المعاملات المشبوهة المتصلة بالاحتيال الذي يسهّل الإنترنت ارتكابه، وذلك لاحتمال تبديد متحصلاته. وتستخدم بعض وحدات الاستخبارات المالية نظامَ تحديد الأولويات لفحص الكم الكبير من تقارير المعاملات المشبوهة والتركيز على أخطر المعاملات المشبوهة، وهي تشمل تقارير المعاملات المشبوهة المتصلة بالاحتيال الذي يسهّل الإنترنت ارتكابه. وتقوم دول أخرى بتدريب الموظّفين في وحدات الاستخبارات المالية التابعة لها على مخاطر غسل الأموال المتعلقة بالاحتيال الذي يسهّل الإنترنت ارتكابه، وهو ما يمكّنهم من فحص وتصنيف تقارير المعاملات المشبوهة الواردة المتعلقة بهذا الاحتيال. وكل هذه التدابير تيسّر قيام وحدة الاستخبارات المالية بإجراء التحليل في سريعًا الوقت المناسب، فيتيح ذلك لإنفاذ القانون متابعةَ حوادث الاحتيال الذي يسهّل الإنترنت ارتكابه بسرعة.

20 انظر مجموعة العمل المالي (يونيو/حزيران 2023) تحديث مستهدف حول تنفيذ معايير مجموعة العمل المالي للأصول الافتراضية ومزودي خدمات الأصول الافتراضية.

المربع 22: تحديد الأولوية في تقارير المعاملات المشبوهة المتصلة بالاحتيال الذي يسهّل الإنترنت ارتكابه وتجميعها

تلقت وحدة الاستخبارات المالية في شيلي أكثر من 1500 تقرير عن المعاملات المشبوهة من 2021 إلى 2022 تتعلق بمخطّط احتيالٍ بمنصة تداول عبر الإنترنت. وللتعامل مع هذا الكم، طبّقت وحدة الاستخبارات المالية في شيلي تقنيات التجميع من أجل التحليل فكشفت أنماطًا معينةً في تقارير المعاملات المشبوهة هذه.

واستخدمت وحدة الاستخبارات المالية أداةَ تنقيبٍ في النصوص بالكلمات المفتاحية والعبارات المعروفة التي كشفتها. فحدّدت بعد ذلك مجموعات جغرافية، وهذا أتاح لها إحالةً مكثّفة ودقيقة الهدف إلى مكتب المدعي العام. وقد مكّن هذا التجميع أن يُكشَف بالتحقيق أنّ الأموال سُحِبت لاحقًا بأجهزة الصراف الآلي، ثم أعطيت إلى شخص مكانةٍ أعلى في هرم جامعة الجريمة المنظمة.

المصدر: شيلي

56. وإلى جانب الكشف، سعت الولايات القضائية إلى زيادة الوعي وتحسين عملية الإبلاغ. فأصدر كثير من الولايات القضائية نوعًا من المبادئ التوجيهية المتعلقة بالاحتيال الذي يسهّل الإنترنت ارتكابه، ونظّمت ندوات تعليمية لموظفي البنوك والقطاعات الأخرى لتعزيز الوعي على مستوى الصناعة بأحدث اتجاهات هذا الاحتيال وتطبيقات غسل الأموال. ويرجى الاطلاع على الملحق (أ) للحصول على جملةٍ من مؤشرات المخاطر التي قد تعين على تعزيز كشف الاحتيال الذي يسهّل الإنترنت ارتكابه. وقد أعدّت وحدات استخبارات مالية في ولايات قضائية أخرى أوراقًا بحثية تحليلية إستراتيجية تدور حول الاحتيال الذي يسهّل الإنترنت ارتكابه. وهذه المبادرات إنما تهدف إلى تعزيز كشف جرائم الاحتيال الذي يسهّل الإنترنت ارتكابه وأنشطة غسل الأموال والوقاية منها من قبل موظفي البنوك الذين في الخطوط الأمامية ...إلخ.

المربع 23: التحليل الإستراتيجي حول بغال المال في الاحتيال الذي يسهّل الإنترنت ارتكابه

ركّز تحليلٌ إستراتيجي أجرته وحدة الاستخبارات المالية الإسبانية على فهم ملف تعريف لبغل مال قد كُشِف، ورد فيه أن شخصًا واحدًا فتح حسابات مصرفية في ثلاث مؤسسات مالية أو أكثر خلال 20 يومًا. وبالاعتماد على المعلومات المستخرجة بين ديسمبر/كانون الأول 2020 وفبراير/شباط 2022 من سجل الحسابات المصرفية، وجدت الدراسة ما يقرب من 40 ألف حسابٍ مصرفيّ آخر مرتبط بنحو 10 آلاف فرد. وإنّ 15% من الحسابات المصرفية التي حُدِّدت وُجِدَ لها ذِكرٌ في قواعد بيانات وحدة الاستخبارات المالية الإسبانية. وقد صُنِّفت هذه الحسابات على أنها عالية المخاطر، وأطلقت دراسة تجريبية بالتعاون مع أربع مؤسسات مالية لتعزيز فهم سمات المخاطر بناءً على هذه الحسابات.

والغرض من الدراسة التجريبية منع الاحتيال الذي يسهّل الإنترنت ارتكابه وغيره من عمليات الاحتيال المحتملة، إضافةً إلى تحسين التعاون مع القطاع الخاص. للدراسة التجريبية غرض آخر، وهو تعزيز قدرة المؤسسات المالية على كشف الثغرات في أنظمتها، والحصول على مزيد من المعلومات حول الاحتيال الذي يسهّل الإنترنت ارتكابه لكشف مزيد من الجرائم ومنعها. وفي آخر المطاف، أفضت الدراسة التجريبية أيضًا إلى تطبيق نظامٍ للتحقّق يستفيد من سجل الحسابات المصرفية لاستباق الكشف عن شبكات غسل الأموال المتعلقة بالاحتيال الذي يسهّل الإنترنت ارتكابه.

المصدر: إسبانيا

2-4 التنسيق والتعاون الداخليَّان

التنسيق بين الجهات المختصّة

57. نظرًا للطبيعة المتداخلة للاحتيال الذي يسهّل الإنترنت ارتكابه، هناك حاجة واضحة إلى تنسيق داخليّ قوي بين الوكالات. ولقد تناولت بعض الولايات القضائية التنسيقَ من خلال نهج إستراتيجي يشمل الحكومة بأسرها ويوجّه ما تتخذه الولاية القضائية من سياسات متصلة بالاحتيال الذي يسهّل الإنترنت ارتكابه. وهذا النهج ينطوي على هيئة شاملة متعدّدة الوظائف، تتألّف من الوزارات الرئيسية عبر قطاعات القضاء والإنفاذ والتنظيم وقطاعَي المعلومات والاتصالات. ويتيح نهج التنسيق للولايات القضائية تحديدَ أهمّ نقاط الضعف واستحداث استجابات سياسية شاملة في القطاعات الرئيسية.

58. يمكن لتنسيق العمليات الداخلية أن يشمل أيضًا الوكالات التقنية لتعزيز أعمال الكشف والتحقيق. وهذا يتضمن:

- تطوير قنوات الاتّصال بين وحدات الاستخبارات المالية والشرطة والمدّعين العامّين لضمان مركزية الإبلاغ، وتسهيل تبادل المعلومات والأدلة، فضلًا عن تعليمات تجميد الأصول ووضع اليد عليها. وقد يشمل ذلك أيضًا استخدام الفرز الآلي للبيانات المُعِينة على تحديد المسائل المحتملة ذات الأهمية والإسراع في تحديد وكالة إنفاذ القانون المناسبة للتحقيق. وهذا التنسيق يخفّف من مضاعفة جهود إنفاذ القانون هدرًا، إذ يمكن لمجرمي الاحتيال الذي يسهّل الإنترنت ارتكابه استهداف الضحايا في أجزاء مختلفة من الولاية القضائية (انظر قسم التحديد الصحيح للمسؤولية أدناه).
- الاستفادة من الخبراء التقنيين في مجال الجرائم الإلكترونية، ولا سيّما في اختراقات الشبكات وغيرها من جرائم البنية التحتية التقنية، إضافةً إلى وكالات حماية الخصوصية. وهذا إنما يعكس الطبيعة المتعدّدة الأوجه للاحتيال الذي يسهّل الإنترنت ارتكابه، ويعكس أهمية الأدلة الجنائية الرقمية (كعناوين بروتوكول الإنترنت والمُعرّفات المرتبطة بنطاقات الإنترنت وما إلى ذلك) في تحديد عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه والنهوض بالتحقيقات في جرائم غسل الأموال.

المربع 24: مركز التنسيق المشترك للشرطة المعنية بالجرائم الإلكترونية

تقود الشرطة الفيدرالية الأسترالية مركز التنسيق المشترك للشرطة المعنية بالجرائم الإلكترونية. وتشمل عضوية مركز التنسيق المشترك للشرطة المعنية بالجرائم الإلكترونية جهات إنفاذ القانون على المستوى الاتحادي وعلى مستوى الولايات، ومحلّلين حكوميين، ومنهم وحدة الاستخبارات المالية الأسترالية، وشركاء الصناعة، كالمحلّلين من البنوك الأسترالية. وإن مركز التنسيق المشترك للشرطة المعنية بالجرائم الإلكترونية:

- ينسّق استجابة الشرطة الأسترالية للجرائم الإلكترونية ذات الحجم الكبير والضرّر الواسع لتحقيق أقصى قدر من التأثير على البيئة الإجرامية،
- ويعزّز تبادل المعلومات الاستخبارية وتطوير الأهداف فيما بين شرطة الكومنولث وشرطة الولايات والأقاليم والصناعةّ،
- وينسّق اشتراك فِرَق العمل مع شركاء الشرطة والصناعة لمواجهة تهديدات الجرائم الإلكترونية ذات الأولوية،
- ويوفر تنسيقًا وطنيًّا لرفع القدرات بصقل المهارات والتدريب المشترك وتطوير الأدوات التعاونية،
- وينشر الاتّساق على المستوى الوطني عبر الوقاية وزيادة الوعي والأنشطة الإعلامية في الصناعة وعامّة الناس.

ولمركز التنسيق المشترك للشرطة المعنية بالجرائم الإلكترونية قدرة وقائية تعمل هي والصناعة والأملاك العامة على مكافحة الجرائم الإلكترونية. ومن أجل دعم مركز التنسيق المشترك للشرطة المعنية بالجرائم الإلكترونية بشكلٍ فعّال، عيّنت وحدة الاستخبارات المالية الأسترالية أيضًا فريقًا لمكافحة الجرائم الإلكترونية المالية، يُركِّز بشكل خاص على توفير المعلومات الاستخباراتية المالية المتعلقة بالجرائم الإلكترونية والجرائم المعتمدة على الإنترنت التي لها ارتباط بالمال، وهي تتضمن

غسل الأموال المتأتية من الاحتيال الذي يسهّل الإنترنت ارتكابه.

وفي يناير/كانون الثاني 2020، ابتدأت الشرطة الفيدرالية الأسترالية عملية دولوس (DOLOS)، ودولوس فرقة عمل متعدّدة الوكالات تقودها الشرطة الفيدرالية الأسترالية[1]، تتصدّى لمجرمي الإنترنت العابرين للحدود الوطنية الذين يرتكبون أو ييسّرون اختراق البريد الإلكتروني التجاري. تعمل دولوس مع الأفراد الأستراليين والشركات الصغيرة والمتوسطة التي استُهدفَت باختراق البريد الإلكتروني التجاري، وتُعطِّل تدفُّق المتحصلات الواردة على عصابات اختراق البريد الإلكتروني التجاري والصادرة عنهم. ومنذ بدء عملية دولوس، طوّرت فرقة العمل تقنياتٍ جديدة أدّت إلى تقليل الضّرر الذي يلحق بالأستراليين والشركات. فبين 1 يوليو/تموز 2022 و30 يونيو/حزيران 2023، حالت عملية دولوس دون فقدان أكثر من 30.6 مليون دولار أسترالي من الضحايا الأستراليين والدوليّين، وذلك من خلال تعطيل نموذج التشغيل المالي الذي يستخدمه المجرمون.

المصدر: أستراليا

1 تضمّ فرقة العمل شرطةً من الأقاليم والولايات، ووكالات استخبارات وأمن سيبراني، ووحدة الاستخبارات المالية، إضافةً إلى القطاع المالي.

الشراكات التشغيلية مع القطاع الخاص

59. سعت الولايات القضائية أيضًا إلى التعاون مع القطاع الخاص بإقامة الشراكات بين القطاعين العام والخاص. ويمكن لهذه الشراكات بين القطاعين العام والخاص أن تُعينَ على تحسين جهود الكشف، وتحديد شبكات غسل الأموال المخفية من خلال تبادل المعلومات التكتيكية، وتعزيز الاستجابة التشغيلية في استرداد الأموال.

المربع 25: مشروع: إجراءات سريعة لمنع عمليات الاحتيال

أطلقت وحدة الاستخبارات المالية في سريلانكا مشروعًا يسمى الإجراءات السريعة لمنع عمليات الاحتيال (RAPS)، وهو مشروع يتصرّف فورًا بمجرد إبلاغ الضحية عن احتمال وقوع الاحتيال الذي يسهّل الإنترنت ارتكابه. والغرض منه هو تعطيل عمليات الاحتيال في النظام المالي السريلانكي، ومن ذلك الاحتيال الذي يسهّل الإنترنت ارتكابه، من خلال الجمع بين وحدة الاستخبارات المالية وموظّفي الامتثال في المؤسسات المالية للكشف سريعًا عن أنشطة الحسابات غير المشروعة التي يستخدمها المجرمون والمتواطئون معهم.

وتتضمن الآلية تحديد بيانات تسجيل دخول المحتالين بناءً على الشكاوى العامة الواردة، ثم تعطى بيانات تسجيل دخول هؤلاء المحتالين لموظفي الامتثال في المؤسسات المالية. وبناءً على هذه المعلومات، تقوم المؤسسات المالية برصد أنشطة حسابات المحتالين المحتملين واتّخاذ الإجراءات المناسبة لتعطيل استخدام النظام المالي بغيةَ منع أي احتيال. ويضاف إلى ذلك أنه تتم مشاركة معلومات المحتالين مع شرطة سريلانكا لإجراء تحقيقات حول الموضوع.

المصدر: سريلانكا

60. في ضوء الزيادة الملحوظة في الاحتيال الذي يسهّل الإنترنت ارتكابه، إضافةً إلى مخاطر غسل الأموال المرتبطة به، أنشأ كثيرٌ من الولايات القضائية مراكز استجابة مركزية في وكالات إنفاذ القانون أو الهيئات التنظيمية لتكثيف الإجراءات ضد هذا الاحتيال وزيادة الوعي العامّ (انظر أيضًا أدناه القسم الخاص بالوحدات المختصّة بمكافحة الاحتيال الذي يسهّل الإنترنت ارتكابه). ومما يعدّ ممارسةً جيدةً أنه يمكن لممثلي المؤسسات المالية ومزوّدي خدمات الأصول الافتراضية أن يكونوا في مواقع مشتركة داخل مراكز الاستجابة المركزية هذه، وهو ما يوفر وصولاً يكاد يكون آنيًّا إلى البيانات المالية وتتبُّعها عبر مختلف الكيانات والقطاعات المالية، ويُسرّع قدرة السلطات المختصة على اعتراض الأموال وتجميدها.

المربع 26: موظفو البنك في موقع مشترك

أنشأت المملكة العربية السعودية غرفة عمليات مشتركة للبنوك. وتتولى هذه الغرفة متابعة ورصد حالات الاحتيال المالي التي قد يتعرض لها عملاء البنوك. وتجمع غرفة العمليات المشتركة كلَّ البنوك والمؤسسات المالية ذات الصلة تحت مظلةٍ واحدة لمعالجة حالات الاحتيال المالي المؤكدة.

وتستضيف البنوك في المملكة العربية السعودية غرفة العمليات المشتركة لتيسير الجهود المشتركة المبذولة لتحقيق استقرار القطاع المصرفي. وتعمل غرفة العمليات المشتركة على مدار الساعة طوال أيام الأسبوع، وغرضها التعاون والتكامل السريعان والفعّالان بين جميع البنوك السعودية للحدّ من تفاقم حالات الاحتيال، وكذلك إتاحة الاستجابة السريعة لشكاوى الاحتيال، واتّخاذ إجراءات فورية لتجنب الأعمال الاحتيالية متى كان ذلك ممكنًا.

المصدر: المملكة العربية السعودية

61. توفر هذه الشراكات أيضًا منصةً مفيدةً لتبادل الممارسات المثلى والتطبيقات المشتركة والمشاركة في وضع التدابير الموصى بها لإحباط النشاط غير المشروع.

المربع 27: شراكة اليوروبول بين القطاعين العام والخاص في الاستخبارات المالية

تعدُّ شراكة اليوروبول بين القطاعين العام والخاص في الاستخبارات المالية (EFIPPP) أولَ آليةٍ عابرة للحدود الوطنية لتبادل المعلومات بين القطاعين العام والخاص لمكافحة غسل الأموال وتمويل الإرهاب. وتجمع هذه الشراكة بين هيئات إنفاذ القانون ووحدات الاستخبارات المالية والكيانات الخاصة من مختلف دول الاتحاد الأوروبي وخارجه.

وقد خصص الفريق العامل المعني بالتهديدات والتطبيقات داخل شراكة اليوروبول بين القطاعين العام والخاص في الاستخبارات المالية مسارات عمل دارت حول موضوعات شتّى منها ما هو عن الاحتيال الذي يسهّل الإنترنت ارتكابه أو متعلق به، وحول طرق عمله المختلفة، بما في ذلك اختراق البريد الإلكتروني التجاري، والاحتيال بالاستثمار، وحسابات بغال المال، وأرقام الحسابات المصرفية الدولية الافتراضية، والأصول الرقمية. وصحيح أنّ هدف هذه الشراكة هو إنشاء تقارير تطبيقية إستراتيجية، ولكنها تتيح أيضًا منصةً لمناقشة تيسير التعاون التشغيلي بين أعضاء الشراكة.

المصدر: اليوروبول

62. قد يختلف تكوين الشراكات بين القطاعين العام والخاص. فما يزال كثير من الولايات القضائية مركّزًا على أصحاب المصلحة التقليديين (وبخاصة البنوك والمؤسسات المالية الأخرى)، ولكن هناك إشراك متزايدة للأعمال والمهن غير المالية المحددة ومزوّدي خدمات الأصول الافتراضية والقطاعات غير التقليدية الأخرى (مثل مشغّلي أعمال الاتصالات ومزوّدي خدمات الإنترنت). والتكوين المحدّد لكل شراكة بين القطاعين العام والخاص معتمدٌ على أهداف الشراكة ومقاصدها.

المربع 28: التعاون مع قطاع الاتصالات

في السنوات الأخيرة، لم تزل الصين تعزّز تقوية مكافحة الاحتيال في شبكات الاتصالات وإدارته، وفي 1 ديسمبر/كانون الأول 2022 طبّقت رسميًا "قانون مكافحة الاحتيال في شبكات الاتصالات لجمهورية الصين الشعبية"، وقد جاء ذلك بضماناتٍ قويّة لسيادة القانون على مكافحة الأنشطة الإجرامية للاحتيال في شبكات الاتصالات وكبحها، وقد كُبِحَت الأعمال الإجرامية ذات الصلة على نحو فعّال.

ويجمع هذا القانون بين سلطات القطاع العام (بما في ذلك وكالات إنفاذ القانون والوكالات المالية ووكالات الاتصالات ومعلومات الإنترنت)، وبين المؤسسات المالية (أي البنوك ومزوّدي خدمات الدفع غير المصرفية)، وبين مشغّلي أعمال الاتصالات ومزوّدي خدمات الإنترنت، وذلك من أجل إنشاء نظامٍ للإنذار المبكر والردع. كما أنه يحدد الضحايا المحتملين فينذر بهم مبكرًا، وهذا يمكّن من اتّخاذ التدابير الرادعة المناسبة سريعًا في الوقت المناسب.

ويمكن للمؤسسات المالية أيضًا استخدام هذا النظام عند فتح الحسابات المصرفية وحسابات الدفع وتقديم خدمات الدفع والتسوية. وهذا النظام إنما يُستخدَم لتعزيز عمليات العناية الواجبة تجاه العملاء ويسمح للمؤسسات المالية باتخاذ تدابير تُخفِّف بها المخاطر من أجل منع استخدام الحسابات المصرفية وحسابات الدفع وما إلى ذلك في أنشطة الاحتيال.

المصدر: الصين

3-4 إستراتيجيات الإنفاذ المحلي المفيدة

63. يبحث هذا القسم في بعض الممارسات الجيّدة وإستراتيجيات الإنفاذ المفيدة التي استخدمتها الولايات القضائية. وتُفيدُ هذه الإستراتيجيات عمومًا مصادر المعلومات التي نوقشت في القسم 4-1 أعلاه، وذلك لتحديد الاحتيال الذي يسهّل الإنترنت ارتكابه وما يتّصل به من غسل الأموال والتحقيق فيه ومنعه على نحوٍ أكثر فعّالية.

64. تشمل إستراتيجيات الإنفاذ المفيدة عادةً وكالات متعدّدة وكيانات من القطاع الخاص. وهذا يعني أن التنسيق والتعاون المحليَّيْن القويَّيْن مطلوبَيْن عادةً لتنفيذ هذه الإستراتيجيات (كما نوقش في القسم 4-2 أعلاه).

التحديد السليم للمسؤولية

65. أبلغت العديد من الولايات القضائية بزيادةٍ في كمّ الخسائر وقضايا الاحتيال الذي يسهّل الإنترنت ارتكابه في السنوات القليلة الماضية. وعلى حين أن بعض القضايا المفردة قد تنطوي على خسائر صغيرة، فإن كمّ عمليات الاحتيال هذه يعني أن إجماليَّ متحصلات الجريمة التي تراكمت عند كلّ عصابة يمكن أن يكون كبيرًا.

66. أشارت عدّة ولايات قضائية إلى أن الكم الكثير لبلاغات الاحتيال الذي يسهّل الإنترنت ارتكابه يجعل تحديد المسؤولية عن التحقيق أمرًا ضروريًا. ومما يعدّ ممارسةً جيّدة أن الولايات القضائية التي لها وكالات مختلفة لمكافحة الاحتيال أو الجرائم الإلكترونية التي تشرف على قضايا الاحتيال الذي يسهّل الإنترنت ارتكابه سَعَتْ إلى تحديد السلطة المختصّة أو السلطات التي تتناول هذه القضايا. وأدخلت ولايات قضائية أخرى تشريعات لتوحيد التحقيقات المُعقَّدة التي تشتمل على ضحايا متعدّدين لنفس العصابة، بحيث تتولى سلطة مختصة واحدة الإشراف على التحقيق بأسره. وإن مثل هذه المبادرات يمنع هدر الجهود التي تبذلها مختلف السلطات المختصة وتمنع إغفال القضايا، فضلاً عن أنها تعالج الطبيعة العابرة للحدود الوطنية للجريمة.

المربع 29: استخدام التكنولوجيا لتحديد مسؤولية التحقيق

أنشأت شرطة هونغ كونغ مركز معالجة الجرائم الإلكترونية وتحليلها (e-Hub) في سبتمبر/أيلول 2022 بهدف تعزيز الفعّالية في تناول البلاغات المتعلقة بجرائم التكنولوجيا والخداع. ويستخدم هذا المركز نظامَ حاسوبٍ محسّنًا لإجراء تحليل الارتباط ضد الأنواع الشائعة من حالات الاحتيال الذي يسهّل الإنترنت ارتكابه، إضافةً إلى تحديده لمجموعات القضايا.

وفي سنة 2022، ارتفع عدد قضايا الخداع بنسبة 45.1% ليصل إلى 27923 قضية، وهو ما يمثل 40% من إجماليّ عدد الجرائم. وكان ما يقرب من 80٪ من حالات الخداع مرتبطًا بالاحتيال الذي يسهّل الإنترنت ارتكابه. وما يزال مزيدٌ من الأشخاص يبلغون عن الاحتيال الذي يسهّل الإنترنت ارتكابه، ومعظم الحالات المبلغ عنها في الإنترنت مرتبط بعضها ببعض، ومثال هذا الارتباط أنها مرتكبة من الجماعة الإجرامية نفسها. فيتم إسناد القضايا المترابطة إلى فريق تحقيق واحد لإجراء تحقيق موحّد، بحيث يمكن تنسيق الموارد على نحو أفضل.

وباستخدام خوارزميات التجميع، يمكن لمركز معالجة الجرائم الإلكترونية وتحليلها تحديد الأنماط وأوجه التشابه في البيانات التي قد لا تكون واضحة على الفور، وذلك لتوسيع فهم نطاق القضايا وطبيعتها. ومن ذلك: الأنواع الشائعة من الأدوات الرقمية الإجرامية وحسابات بغال المال المستخدمة، وكيفية التخطيط للاحتيال الذي يسهّل الإنترنت ارتكابه وتنفيذه وإخفائه.

المصدر: هونغ كونغ، الصين

وحدات مخصّصة لمكافحة الاحتيال الذي يسهّل الإنترنت ارتكابه وما يتّصل به من غسل الأموال

67. أنشأ كثير من الولايات القضائية من أجل تعزيز قدرات مكافحة غسل الأموال وتمويل الإرهاب في مواجهة المشهد الإجرامي المتطوّر وحدةً أو فريقًا عاملاً محددًا للتحقيق في الاحتيال الذي يسهّل الإنترنت ارتكابه وغسل الأموال المتصل به. وخصّصت هذه الولايات القضائية مواردَ إضافيّةً لتعزيز القدرات في مجال التحقيق المالي، وجمع المعلومات الاستخبارية، وتدريب وكالات إنفاذ القانون، وبناء قدرات القطاع الخاص. وتعمل هذه الوحدات المركزية على توحيد الخبرة في مجال مكافحة الاحتيال الذي يسهّل الإنترنت ارتكابه بين أجهزة إنفاذ القانون وجعلها أكثر قدرةً على تعطيل عمليات هذا الاحتيال وتتبُّع الأموال المغسولة واسترداد المتحصلات المتصلة بها.

68. اتّفقت الولايات القضائية على أن فوائد مثل هذه التجهيزات متعدّدة الجوانب. فإن توحيد جميع قضايا الاحتيال الذي يسهّل الإنترنت ارتكابه من خلال وحدةِ إنفاذٍ واحدةٍ يتيح تحليلًا أفضل ونشرًا لتحليلات البيانات وتحليلَ ارتباط الشبكة، ويفيد كل ذلك بتحديد العصابات. كما يمكن أن تكون بمنزلة نقطةِ اتّصالٍ منفردة لأصحاب المصلحة في القطاع الخاص ونظرائهم الأجانب، وأن نعين على تطوير العلاقات الاستراتيجية على المدى البعيد. وهذا يعزز جهود التدخُّل التي تبذلها سلطات إنفاذ القانون، مثل تعطيل خطوط الهاتف، وإزالة الألقاب والإعلانات المشبوهة عبر الإنترنت، وتحسين نتائج استرداد الأموال.

المربع 30: المركز الوطني للاستجابة للاحتيال

المركز الوطني للاستجابة للاحتيال في ماليزيا هو استجابةٌ متعدِّدة الأوجه تجمع جملةً متنوعةً من الموارد والخبرات من المركز الوطني لمكافحة الجرائم المالية، ومن الشرطة الملكية الماليزية، ومن البنك المركزي، ومن كياناتٍ أخرى في القطاعين العام والخاص.

وهذا المركز هو مكان تُجمَّعُ فيه معلومات الاحتيال الواردة من مصادر مختلفة فيُفيدُ تحليلَ الشبكة لتحديد شبكات بغال المال وغسل الأموال. فتقوم كيانات القطاع الخاص، بما في ذلك المؤسسات المالية، بتتبُّع الأموال من طبقة إلى طبقة أخرى ثمّ تحجز حسابات بغال المال. ثم تحقيق الشرطة الملكية الماليزية في القضية بشكل أكبر وتتّخذ إجراءات إنفاذ القانون، كإصدار أمر تجميد الحسابات.

المصدر: ماليزيا

تعزيز الوصول إلى المعلومات المالية

69. نظرًا للأثر الهائل والفوري لقضايا الاحتيال الذي يسهّل الإنترنت ارتكابه، فإن الوصول السريع إلى المعلومات المالية والمصرفية أمرٌ بالغ الأهمية، يعين على تعجيل التحقيق وتتبُّع متحصلات هذا الاحتيال. وقد استخدمت بعض الولايات القضائية التكنولوجيا لمواكبة التدفُّقات السريعة لمتحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه، وكثيرًا ما تعاونت مع القطاع الخاص في هذه العملية. وتعتمد ولايات قضائية أخرى على السجلات المركزية أو يضعون قواعد بيانات تسهّل عملية استرجاع المعلومات. وهذه ممارساتٌ جيّدة، تعتمد عادةً على إنشاء منصة مركزية تجمع بين عديدٍ من أصحاب المصلحة لتبادل المعلومات على نحو أسرع.

- **استرجاع المعلومات باستخدام التكنولوجيا:** من أجل تمكين المؤسّسات المالية من تقديم المعلومات ذاتِ الصلة سريعًا إلى سلطات إنفاذ القانون، قد يكون من المفيد للسلطات المختصة داخل الولاية القضائية الاتّفاق على حقول البيانات التي قد تكون متصلة بتحقيقاتها. فإن إصدار طلبات متنوعة يتطلب كل منها استجابةً مخصّصةً من المؤسسة المالية المعنية قد تستغرق معالجتها في القطاع الخاص وقتًا طويلاً. ومما يعدّ ممارسةً جيّدة أن جهات إنفاذ القانون في بعض الولايات القضائية طوّرت نموذجًا موحّدًا يشتمل على حقول البيانات المتفق عليها مسبقًا، تطلبها هذه الجهات من المؤسسات المالية. ويمكن بعد ذلك تصنيف الطلبات وإرسالها إلى المؤسسات المالية على دفعات وتكون بحيث يمكن قراءتها آليًّا. ويمكن للمؤسسات المالية أيضًا تقديم استجابات للطلبات القانونية رقميًا إلى جهات إنفاذ القانون، وهذا يتيح تحليل البيانات على نحو أكثر كفاءة.

المربع 31: تعزيز أتمتة العمليات الآلية لتسريع الوصول إلى السجلات المالية التي تحتفظ بها المؤسسات المالية

يُعدُّ الوصول السريع إلى المعلومات المصرفية والمالية أمرًا بالغ الأهمية للاعتراض الفعّال واسترداد الأموال. وتعزّز سنغافورة أتمتة العمليات الآلية لتحصل على المعلومات المصرفية في مدةٍ وجيزة بالقياس إلى الوقت الذي كانت تستغرقه سابقًا. وتُقدَّم الطلبات الآن إلكترونيًا إلى البنوك عبر نموذج موحّد. وتقوم البنوك بأتمتة عملية استرجاع المعلومات المالية ومن ثم إرسالها ثانيةً إلى وكالات إنفاذ القانون إلكترونيًّا. ويمكن أيضًا استخدام البيانات الإلكترونية على الفور في التحليل الذي تجريه وكالة إنفاذ القانون.

وقد أدّت هذه العملية إلى تقصير زمن التنفيذ بنسبة تصل إلى 97%، فنتج عن ذلك إجراءُ تحقيقاتٍ أكثر كفاءةً. وتُتَاح المعلومات اليوم في صيغة رقميّة جاهزةٍ للتحليل. أما البنوك، فقد أدت هذه المبادرة إلى تقليل كثير مما تتكبده من الكلفة بإلغاء إجراء العمل يدويًّا. وبالمثل، مكّنت المبادرة من استخراج البيانات للبنوك بمن خلال عملياتها الآلية التي يمكن استخدامها لزيادة الكشف عن شبكات غسل الأموال المخفية.

المصدر: سنغافورة

- **تيسير تتبع الأصول عبر المؤسسات المالية:** تؤدي المعاملات العابرة والتنقّل بين الحسابات عبر العديد من المؤسسات المالية إلى زيادة جهود تتبّع إنفاذ القانون، إذ يتطلب الأمر وقتًا لجمع المعلومات من المؤسسات المالية المعنية، ولتنقية طبقات المعاملات وتحديد مصدر الأموال ووجهتها النهائية. وقد يكون هذا أمرًا صعبًا

لأن المعاملات سريعة. ومن الممارسات الجيّدة تطوير منصات تُيسِّر التتبُّع السريع وتبادل المعلومات عبر مختلف المؤسسات المالية لاعتراض المتحصلات غير المشروعة.

المربع 32: نظام إبلاغ المواطنين عن الاحتيال الإلكتروني المالي وتدبيره

هو نظام يعمل عبر الإنترنت طُوِّرَ من قبل المركز الهندي لتنسيق مكافحة الجرائم الإلكترونية للإبلاغ السريع عن عمليات الاحتيال المالي عبر الإنترنت ومنع تدفُّق متحصلات الاحتيال عبر القطاعات المالية. وقد أدمج النظام وكالات إنفاذ القانون في جميع أنحاء البلاد والكيانات المالية (أي البنوك والمَحَافظ ومجمعّات الدفع وبوابات الدفع ومنصات التجارة الإلكترونية وما إلى ذلك) مع العمل جنبًا إلى جنب واتّخاذ إجراءات فورية بشأن الشكاوى المبلغ عنها في هذا النظام. وفي الوقت الحاضر، فإن جميعَ وكالات إنفاذ القانون في الولايات والأقاليم الاتحادية و243 كيانًا ماليًا مشتركةٌ في الوحدة.

وبمجرد قيام الضحية بإبلاغ وكالة إنفاذ القانون عن عملية احتيال، يتم تسجيل تفاصيل المستفيد من المعاملة الاحتيالية وتقديمها إلى نظام إبلاغ المواطنين عن الاحتيال الإلكتروني المالي وتدبيره في هيئة تذكرة. ثم تُرفَع هذه التذكرة إلى الجهة المالية المعنية (البنك، أو محفظة الدفع أو ما إلى ذلك)، وهي سترى ترى التذكرة على لوحة التحكم في نظامها. ويقوم الكيان بالتحقق مما إذا كانت الأموال التي استلبت بالاحتيال ما تزال موجودةً في الحساب، ثم يحجزها. وإذا تم تبديد الأموال بإرسالها إلى كيان آخر، فستُرفَع التذكرة إلى طبقة تالية من الكيان. وتتكرر العملية حتى تُعتَرَض الأموال. فإذا سُحِبت الأموال، فستقوم المؤسسات المالية بملء تفاصيل السحب لاتخاذ مزيد من الإجراءات من جانب وكالات إنفاذ القانون.

لقد كان النظام فعالاً للغاية في منع المعاملات الاحتيالية من الوقوع في أيدي المحتالين. ومنذ إنشاء هذا النظام في أبريل/نيسان 2021، تمكن من اعتراض أكثر من 6.02 مليار روبية هندية (أي نحو 66.1 مليون يورو).

المصدر: الهند

- **الاستفادة من السجلات المركزية:** تتيح سجلات البنك المركزي لوكالات إنفاذ القانون الوصول السريع إلى المعلومات المصرفية الأساسية وتعين على تسريع تحقيقات الاحتيال الذي يسهّل الإنترنت ارتكابه. وتسمح هذه المعلومات لوكالات إنفاذ القانون بالتحقّق من البنوك التي يكون للمشتبه به فيها حسابات، أو من هوية صاحب الحساب. وذلك إنما يعين على تسهيل استرجاع المعلومات من خلال السماح لوكالات إنفاذ القانون بتوسيع نطاق تحقيقاتها مبكرًا وقَصْر التركيز على المؤسسات المالية التي يكون للمشتبه به فيها حسابات.

المربع 33: تحديد حسابات بغال المال المخفية

قُدِّم تقرير في مالطا عن المعاملات المشبوهة ضد بغل مالٍ مشتبه به بعد سلسلة من المعاملات المشبوهة لمستفيدين مختلفين. فتم تحويل الأموال إلى العديد من البنوك المحلية والدولية المرتبطة بعملية احتيالٍ بعلاقة غرامية مشتبه بها.

فسمحت عمليات البحث في سجل حسابات البنك المركزي الوطني لوحدة الاستخبارات المالية على الفور بتحديد حسابٍ نشطٍ آخر يملكه الشخص المشتبه به في بنك مختلف. وقد تمكنت وحدة الاستخبارات المالية من الإسراع في رسم صورة شاملة ونطاقٍ للتحليل المالي الإضافي المطلوب. وقد ساعد هذا في آخر المطاف وحدةَ الاستخبارات المالية على سرعة تحديد القواسم المشتركة لمزيدٍ من عمليات غسل الأموال مع أفراد أجانب آخرين.

المصدر: مالطة

- **وضع قواعد بيانات لتبادل المعلومات فيما بين مؤسسات القطاع الخاص:** في حالات الشبكات المحترفة لغسل الأموال، قد تكون كثير من حسابات بغال المال معروفةً أو مشتبهًا بها كجزء من عمليات احتيال سابقة (مثل العلاقة الغرامية واليانصيب والتوظيف) أو من أنشطة الاستيلاء على الهوية. وهناك أيضًا تداخلات مماثلة في البيانات والعمليات المستخدمة لتحديد الاحتيال والمستخدمة لتحديد شبكات بغال المال. وممّا يعدّ ممارسةً جيّدة أنبعض الولايات القضائية سعت إلى مركزية البيانات التي تشمل قواعد بيانات مكافحة الاحتيال ومكافحة غسل الأموال لتحديد شبكات أعمق لغسل الأموال عبر مختلف المؤسسات المالية من أجل منع الاحتيال وتعزيز استرداد الأموال.

المربع 34: قاعدة بيانات مركزية في ما بين مؤسسات القطاع الخاص

وافقت البرازيل مؤخرًا على قرار مُلزم يُنشأُ بموجبه قاعدةٌ للبيانات تُجمّع المعلومات المتعلقة بالاحتيال (بما في ذلك المحاولات) من جانب جميع المؤسسات المالية ومؤسسات الدفع. والذي طبّق قاعدة البيانات هذه هو البنك المركزي البرازيلي، ومن المتوقع أن يبدأ العمل في نوفمبر/تشرين الثاني 2023.

وينص القرار على أن مشاركة المعلومات حول عمليات الاحتيال (بما في ذلك المحاولات) أمرٌ مُلزمٌ للمؤسّسات، ويُحدّد الحد الأدنى من المعلومات التي يجب مشاركتها. ومن ذلك تحديد هوية الأشخاص المتورّطين في ارتكاب الاحتيال (بما في ذلك بغال الأموال)، والمؤسسة (أو المؤسسات) المالية المشاركة، والحساب (أو الحسابات) المستخدمة. ويهدف النظام إلى تيسير تبادل المعلومات بين مؤسسات القطاع الخاص بهدف منع الاحتيال ومكافحته واسترداد متحصلات الاحتيال غير المشروعة.

المصدر: البرازيل

ردع بغال المال

70. لبغال المال دورٌ مهمٌّ في شبكات غسل الأموال المتصلة بالاحتيال الذي يسهّل الإنترنت ارتكابه، كما نوقش سابقًا. وبغال المال يُعيَّنون ويُستخدَمون من خلال عدد لا يحصى من التقنيات. وبحسب كيفية تعيينهم وما إذا كانوا قد تعرّضوا للخداع أو الاستغلال عن غير قصد، يمكن أن يكون لهم مستويات متفاوتة من المعرفة والمشاركة في المخطط الأساسي للاحتيال الذي يسهّل الإنترنت ارتكابه (انظر القسم 2-3 أعلاه).

71. ثمّ إن السلطات المختصة قد تواجه تحديات في توجيه تهم غسل الأموال لهم. فقد يصعب الإتيان بأدلة كافية لإثبات النية الجرمية لبغل المال في غسل الأموال (والمقصود بها مستوى إدراكه بمشاركته في عملية غسل الأموال). ولمعالجة هذه المشكلة، أصدرت بعض الولايات القضائية تشريعاتٍ لخفض حد النية الجرمية المطلوب في جرم غسل الأموال، مثل خفض حد "المعرفة" إلى حد "الشك".

المربع 35: الفقرة 3 من المادة 9 من اتفاقية وارسو في مجلس أوروبا

إنّ من أهمّ الأمور في الملاحقة الجنائية الفعّالة لجريمة غسل الأموال هي الحاجة إلى إثبات النية الجرمية، ومعناها أن غاسل الأموال كان على علم بأن المتحصلات التي تناولها هي متحصلات جريمة. وفي قضايا غسل الأموال المعقّدة التي يتورط فيها غاسلو أموال محترفون، ينكر المدعى عليه عادةً أن له علمًا راسخًا بأن الأموال التي تناولها كانت من متحصلات الجريمة. ومن ثمّ فإن إثبات أن "الركن المعنويّ" لجرم المدعى عليه قد اكتمل ووصل إلى الحد المطلوب هو من أصعب المهام في إثبات جريمة غسل الأموال.

وإذ قد كان صائغو اتفاقية وارسو مدركين لصعوبة إثبات النية الجرمية، أدخلوا عناصر جديدة في المادة 9، حيث هو منصوص على جريمة غسل الأموال. وبصرف النظر عن العناصر المُضمَّنة أصلاً في اتفاقيَّتَي فيينا وباليرمو، فإن الفقرة 3 من المادة 9 من اتفاقية وارسو زادت عليهما ونصّت على أن جرم غسل الأموال يقع بمجرّد اشتباه الجاني بأن المتحصلات قد تأتّت عن جريمة أو كونه جديرًا بأن يفترض ذلك.

المصدر: لجنة الخبراء المعنية بتقييم تدابير مكافحة غسل الأموال وتمويل الإرهاب

72. تعاملت ولايات قضائية أخرى مع التحدي الذي يُمثّله بغال المال عمومًا عن طريق التثقيف العام وتوعية بغال المال المحتملين. وقد بُثّت حملات عالمية على وسائل التواصل الاجتماعي، مثل حملة وسم #DontbeaMule (أي لا تكن بغلًا) التي تدعمها اليوروبول، وحملة وسم #YourAccountYourCrime (أي حسابك إذًا هي جريمتك) التابعة للإنتربول، ومن الممكن أن تكون أمثال هذه الحملات منصاتٍ مفيدةً لتنسيق الوعي الدولي ضد أنشطة بغال المال، ولا سيّما عندما يَسْهُلُ غسلُ الأموال عن طريق بغال المال عبر الحدود. ثم إنه يمكن أن يؤدي التعاون مع القطاع الخاص إلى تحقيق أقصى قدر من التأثير ومن نتائج هذه الجهود المبذولة للتوعية. ويمكن للسلطات أيضًا الاستفادة من آليات الكشف الحالية (أي تقارير المعاملات المشبوهة وبلاغات الضحايا) لتحديد بغال المال المحتملين الذين ربما تعاملوا مع متحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه. كما يمكن للتوعية والتحذيرات الدقيقة الأهداف أن تنصح بغال المال المحتملين بالامتناع عن تكرار مثل هذا السلوك في المستقبل. ويمكن أيضًا الاستفادة من سجلّات التوعية أو التحذيرات السابقة واستخدمها كدليلٍ مفيد في تحديد النية الجرمية لغسل الأموال في حالة معاودة الإجرام.

4-4 الوقاية والعرقلة

73. نظرًا إلى سرعة تبديد الأموال، عملت كثير من الولايات القضائية على استكشاف مبادرات لمنع وقوع الاحتيال الذي يسهّل الإنترنت ارتكابه وغسل الأموال المتّصل به. ومثل هذا النهج يقلل الربح الإجمالي لعصابات الاحتيال الذي يسهّل الإنترنت ارتكابه، ويخفف كثيرًا من تخصيص الموارد في المراحل التنفيذية، ابتداءً من التحقيق إلى إدارة الضحايا.

التثقيف العام والتوعية

74. يمكن اعتمادُ نهجٍ وقائيٍّ بتثقيف الجمهور وزيادة اليقظة ضد الاستغلال، ومن ذلك حملات التوعية الوطنية التي تدعو إلى محو الأمية الإلكترونية. ولدعم هذا الهدف، استفادت بعض الولايات القضائية من التكنولوجيا فأطلقت حملات إعلامية للمواطنين لمساعدتهم على كشف عمليات الاحتيال، وزيادة الوعي بالعلامات المريبة، والحث على بلاغات الضحايا.

المربع 36: الاستفادة من التكنولوجيا في التوعية العامة بشأن الاحتيال الذي يسهّل الإنترنت ارتكابه

أطلقت شرطة هونغ كونغ محركَ بحثٍ شاملاً عن عمليات الاحتيال والمزالق، وهو سكاميتر (Scameter) في سبتمبر/أيلول 2022. والغرض من هذا التطبيق مساعدة الجمهور في تحديد عمليات الاحتيال والمزالق عبر الإنترنت.

فحين يرد على الناس مكالمات مشبوهة، وبائعين مشبوهين عبر الإنترنت، وطلبات صداقة غير المرغوب فيها، ورسائل توظيف عشوائية، ومواقع استثمار احتيالية مشتبه بها، وما شابه ذلك، يمكنهم إدخال اسم حساب المحتال المشتبه به أو رقم حسابه، ورقم حساب الدفع الخاص به، أو رقم هاتفه، أو عنوان بريده الإلكتروني، أو عنوان موقعه في الإنترنت ...إلخ، وذلك لتقدير مخاطر الاحتيال والأمن الإلكتروني.

وتأتي بيانات سكاميتر وتقديراته من مصادرٍ شتّى موثوق بها، ومنها البلاغات العامة المقدمة إلى الشرطة، والمعلومات المقدمة من المنظّمات، وقاعدة بيانات أرقام الهواتف المشبوهة، إضافةً إلى قاعدة البيانات والتحليل الآنية من شركات أمن المعلومات.

المصدر: هونغ كونغ، الصين

الأمن والضوابط في مكافحة الاحتيال لتحقيق نتائج مكافحة غسل الأموال وتمويل الإرهاب

75. بدأت تجارب القطاعين العام والخاص تُظهِر أنّ عمليات مكافحة الاحتيال ومكافحة غسل الأموال يكمّل بعضهما بعضًا. ويتضمّن ذلك الاستفادة من التكنولوجيا لمساعدة المستخدمين في رفض تلقّي الرسائل الاحتيالية تلقائيًا، والعمل مع القطاع الخاص لإجراء مسح أفقي لاستباق التخفيف من اتجاهات الاحتيال الناشئة، وإنشاء ميزات وضوابط وقواعد أمان للحسابات، إضافةً إلى إنشاء رسائل تحذيرية في برامج مكافحة الفيروسات تُنذِرُ بمواقع التصيُّد المحتمل (انظر الملحق ب الذي جُمِعت فيه أمثلة جيّدة عن كيفية اعتماد الهيئات التنظيمية المالية لمتطلبات مكافحة الاحتيال إلى جانب اعتمادها لضوابط مكافحة غسل الأموال وتمويل الإرهاب).

76. ومن الممارسات الجيّدة الأخرى تشجيع المؤسسات المالية على اعتماد رصد المعاملات آنيًّا لتحديد الأنشطة الاحتيالية أو غير المشروعة آنيًّا ومنعها. لأنه برصد المعلومات غير الطبيعية لصاحب الحساب (كالعناوين الحقيقية، وعناوين بروتوكول الإنترنت، وعناوين البريد الإلكتروني، وأرقام الهواتف المحمولة وما إلى ذلك) والمعاملات رصدًا آنيًّا، يمكن للمؤسسات المالية تحديد أي نشاط غير عادي أو مشبوه والتحقيق فيه والإبلاغ عنه بسرعة.

77. يُعدُّ رصد المعاملات آنيًّا، وهو ما يتضمَّن استخدام برامج وخوارزميات متطورة في رصد المعاملات المالية، مفيدٌ لكشف الاحتيال الذي يسهّل الإنترنت ارتكابه ومنعه. فنظرًا إلى تدفق المعلومات الناجم عن الرقمنة قد يصعب كشف هذا الاحتيال بالعمليات اليدوية. ويمكن أن يُعين رصد المعاملات آنيًّا المؤسسات المالية على تحديد أنماط النشاط المشبوه والتحقيق فيها عبر حسابات أو معاملات متعددة، حتى لو لم تكن تلك الحسابات أو المعاملات مرتبطة ارتباطًا مباشرًا، وهذا مما يمنع الجرائم في المستقبل.[21]

إزالة الأدوات الإجرامية

78. لمّا كان الاحتيال الذي يسهّل الإنترنت ارتكابه يمكن أن يُرتَكَب من خلال القطاعات غير التقليدية (انظر القسم 3-3 أعلاه)، عزَّزت بعض الولايات القضائية الوقايةَ من الاحتيال وضوابطَه في هذه القطاعات. ومن ذلك أنها استهدفت أدوات الاحتيال الذي يسهّل الإنترنت ارتكابه، مثل إغلاق خطوط الهاتف المحمول وصفحات الويب الاحتيالية التي يستخدمها المجرمون، وغربلة رسائل التصيُّد وروابط الإنترنت الضارّة، وما إلى ذلك.

21 لمزيد من المعلومات حول كيفية استخدام التكنولوجيا في مكافحة غسل الأموال وتمويل الإرهاب، انظر مجموعة العمل المالي (يوليو/تموز 2021) فرص وتحديات التكنولوجيات الجديدة لمكافحة غسل الأموال وتمويل الإرهاب

المربع 37: إزالة المواقع المشبوهة وحملات التصيُّد

تتَّبع وكالات إنفاذ القانون والسلطات التنظيمية في المملكة العربية السعودية نهجًا تعاونيًا مع مزوّدي خدمات الاتصالات، وذلك لتعزيز قدرتها بشكل كبير على التنبُّؤ بالأحداث الاحتيالية ومنعها وكشفها والاستجابة لها على نحوٍ فعّال. ولمكافحة الأدوات الإجرامية، فرضت الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية شروطًا شديدةً لحماية العلامة التجارية مع تركيزها على مكافحة المواقع المستنسخة ورسائل التصيُّد على منصات التواصل الاجتماعي. ويُضاف إلى ذلك أن البنك المركزي السعودي (ساما) أنشأ أطرًا قويةً للأمن السيبراني ثم لمكافحة الاحتيال على الترتيب، وذلك مع تحديده لمتطلبات رقابة أساسية إلزامية للكيانات الخاضعة للرقابة. ويهدف هذا الإطار إلى استباق الحماية ضد تهديدات الاحتيال الناشئة، ومن ثمّ ضمان استقرار القطاع المالي في المملكة وحمايته.

ومن الجوانب الهامّة جدًّا لهذه المتطلبات الوطنية والتنظيمية هو استباق رصد المنظّمات للأدوات الإجرامية. ومن ذلك الرصد المستمرّ لأنشطة الاحتيال المحتملة، كمواقع الإنترنت المشبوهة وحملات التصيُّد، وذلك بتقنيات متطوّرة وتدابير حماية العلامة التجارية التي تنفذها المؤسسات. فعند كشف هذه الأنشطة يُبلَّغ عنها فورًا إلى السلطات المختصة. ويضمن الإبلاغ السريع اتّخاذ إجراءات سريعة للتحقيق في العمليات الإجرامية وإيقافها، وهذا يمنع زيادة الضّرر ويقلّل من تأثير الأحداث الاحتيالية.

المصدر: المملكة العربية السعودية

منع تبديد الأصول

79. لقد وجد كثير من الولايات القضائية أن أحد أصعب الجوانب في تحقيقات الاحتيال الذي يسهّل الإنترنت ارتكابه هو السرعة الشديدة لغسل متحصلات هذا الاحتيال. وهناك إجماعٌ على أنه من الأهمية بمكان أن تتمكن السلطات المختصة من التدخل سريعًا للوصول إلى متحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه قبل أن تتبدّد من الحسابات المصرفية المختلفة. وطبّقت الولايات القضائية تدابير شتّى لاسترداد الأموال المرتبطة بالاحتيال الذي يسهّل الإنترنت ارتكابه على نحوٍ أكثر فعّالية (انظر القسم 5-1 أدناه).

80. قد تكون هناك أيضًا فوائد لإشراك الممثّلين الرئيسيين للقطاع المالي الخاص في تيسير وتشجيع اعتراضهم الاستباقي للأموال غير المشروعة بمجرّد تلقّي إشعارٍ بالاحتيال من العميل الضحية، قبل أن تتّصل بهم السلطات المختصة. ويشمل ذلك تبادلَ المعلومات بين المؤسّسات المالية المحلية والأجنبية أو مزوّدي خدمات الأصول الافتراضية (انظر أيضًا المربع 41 أدناه).

38: نشرة مجموعة إيغمونت بشأن الاحتيال باختراق البريد الإلكتروني التجاري

في يوليو/تموز من سنة 2019، أصدرت مجموعة إيغمونت نشرةً لتنبيه وحدات الاستخبارات المالية الأعضاء وولاياتها القضائية بالتهديد المتزايد الذي يشكله الاحتيال باختراق البريد الإلكتروني التجاري، فشاركتهم بالسيناريوهات الرئيسية ومؤشرات المخاطر المرتبطة بهذا الاختراق. وذكرت النشرة أيضًا كيف يمكن أن يكون للمؤسسات المالية دورٌ مهمٌّ في تحديد الاحتيال باختراق البريد الإلكتروني التجاري ومنعه والإبلاغ عنه بتعزيز التواصل والتعاون بين وحدات مكافحة غسل الأموال الداخلية، والأعمال التجارية، والوقاية من الاحتيال، والأمن الإلكتروني.

وللمساعدة في التحقيق في حوادث الاحتيال باختراق البريد الإلكتروني التجاري واسترداد أموال الضحايا، نُصِحَت المؤسسات المالية المستفيدة التي تلقّت معلومات تفيد بتنفيذ تحويل احتيالي إلى أحد حسابات عملائها (كرسالة استرجاع تحويل بنظام سويفت) بأن لا تُنفِّذ أي معاملات يمكن أن تؤدي إلى فقدان الأموال والاتّصال بسلطات إنفاذ القانون أو وحدة الاستخبارات المالية لتقدير صحّة المعاملة المستلمة.

المصدر: مجموعة إيغمونت

5 التعاون الدولي واسترداد الأموال

81. قد ذكرنا سابقًا أن الولاية القضائية التي يقع فيها الاحتيال الذي يسهّل الإنترنت ارتكابه (أي مكان وجود الضحية عمومًا) تميل إلى الاختلاف عن الولاية القضائية التي يقع فيها غسل المتحصلات. وهذا يمكن أن يؤدي إلى تحديات تعترض التحقيقات عبر الحدود والتعاون الدولي الفعّال للحصول على المعلومات والأدلة، وتفكيك عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه، واسترداد المتحصلات غير المشروعة. ومثال ذلك أن الولاية القضائية التي غُسِلت فيها متحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه قد تواجه مصاعب في تحديد كلّ ضحية مرتبطة بحساب غسل الأموال فقد يمكن أن يكون الضحايا منتشرين عبر ولايات قضائية متعدّدة.

82. ومما يزيد الأمر تعقيدًا الطبيعة غير المركزية للاحتيال الذي يسهّل الإنترنت ارتكابه. فربما انعدم الاتفاق في أولويات التعاون الدولي الخاصة بكل ولاية قضائية، ومثال ذلك في الحالات التي يقوم فيها ضحايا الولاية القضائية -أ- بتحويل الأموال إلى الولاية القضائية -ب-، ولكن ضحايا الولاية القضائية -ب- موجودون في الولاية القضائية -ج- (أي أن -أ- قد تعطي الأولوية للتعاون مع -ب-، ولكن -ب- قد تعطي الأولوية للتعاون مع -ج-). كما أن الحاجة إلى إشراك العديد من أصحاب المصلحة والشركاء، من القطاعين العام والخاص، في الخارج تصعّب تحديد الأموال غير المشروعة وتتبُّعَها.

- تستخدم عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه شتّى الخدمات المالية وفئات الأصول. ويمكن إجراء المعاملات على نحو يكاد يكون فوريًّا عبر الحدود بين مختلف مزوّدي الخدمات والقطاعات. وهذا إنما يصعّب تتبُّعَ تحويلات الأموال وعزوِها إلى أصحابها.
- يُرجَّح أيضًا أن تُوزّع الأدلة الجنائية الرقمية ذات الصلة عبر ولايات قضائية مختلفة، وهو ما يجعل من الصعب تجميع صورة كاملة واضحة عن كيفية عمل العصابات الإجرامية وغسلها المتحصلات. ومما يزيد الأمر تعقيدًا أن الأدلة الجنائية الرقمية متقلّبة، ويمكن أن تتبدَّد بسهولة إن لم تُحفَظ سريعًا.

83. يستغرق التعاون الرسميّ عادةً وقتًا طويلاً، ومن ذلك المساعدة القانونية المتبادلة. ونظرًا لسرعة الجرائم الرقمية وأنشطة غسل الأموال المرتبطة بها (حيث يمكن تبديد الأدلة سريعًا إذا لم تُحفَظ)، فإن الاعتماد على التعاون الرسميّ قد يقلّل الفعّالية كثيرًا. ولكي تبقى السلطات المختصة نبيهةً في تقديم المساعدة عبر الحدود لكبح النشاط الإجرامي للاحتيال الذي يسهّل الإنترنت ارتكابه، فإنها تعتمد على نحوٍ متزايد على آليّات التعاون غير الرسميّة من خلال تبادلها للمعلومات مباشرةً مع نظيراتها الأجنبية. ويمكن أن يحدث ذلك على مستوى أجهزة إنفاذ القانون أو وحدة الاستخبارات المالية من خلال قنوات مختلفة، ومن هذه القنوات شبكة إيغمونت الآمنة وشبكة الإنتربول (I-24/7)، ويضاف إلى ذلك شبكاتٌ غير رسمية أخرى كشبكة كامدِن المشتركة بين الوكالات لاسترداد الموجودات (CARIN) والشبكات الإقليمية المشتركة بين الوكالات لاسترداد الموجودات (ARINs).

المربع 39: اعتراض متحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه من خلال شبكات غير رسمية متعدّدة الأطراف

تُكثِرُ سلطات التحقيق الفرنسية استخدام شبكات غير رسمية لمكافحة اشتداد الاحتيال الذي يسهّل الإنترنت ارتكابه، ومن هذه الشبكات الشبكة الفرعية للمكاتب الأوروبية لاسترداد الموجودات (AROs) التابعة لشبكة كامدِن المشتركة بين الوكالات لاسترداد الموجودات (CARIN)، وذلك من أجل التعاون الدولي الفعّال وما يتّصل به من استرداد الأموال. ويعمل مكتب الفرنسي لاسترداد الأموال عن كثب مع أعضاء هاتين الشبَّكَتين، وهذا يتيح تبادل المعلومات بسرعة عبر ولايات قضائية متعددة بين وكالة إنفاذ القانون ووحدة الاستخبارات المالية المتخصِّصتَين في تتبُّع الأموال الجنائية وضبطها ومصادرتها، ولا سيّما في حالات الطوارئ، ففيها يُستجابُ للطلبات في 8 ساعات. ويُمكّن هذا التعاون من حِفْظ الأموال بسرعة في حساب الوجهة المُحدَّد في البداية، وجميع الحسابات اللاحقة التي أُرسِل إليها للتمويه.

ومثال ذلك أنه في سنة 2022 اتّصل المكتب الفرنسي لاسترداد الأموال بالمكتب السلوفاكي لاسترداد الأموال بشأن تحويل مصرفي احتيالي قيمته 1,875,000 يورو من جيب الشركة الفرنسية الضحية، وطلب تجميد الأموال في الحساب المصرفي المستفيد في سلوفاكيا. فأدت التبادلات بين مكتبي استرداد الأموال إلى تجميد الأموال، وأتاحت للسلطات السلوفاكية الحصول على جميع المعلومات المطلوبة لإعداد طلب التجميد في القضاء وتنفيذه. وفي آخر المطاف، جُمِّد مبلغ 1,874,907 جنيهًا إسترلينيًا وأُعِيد بعد ذلك إلى الشركة الضحية.

المصدر: فرنسا

84. ولتحقيق أقصى فعّالية في التحقيق في غسل الأموال المتصل بالاحتيال الذي يسهّل الإنترنت ارتكابه واسترداد المتحصلات، ينبغي أن يكون للتعاون تركيز متعدّد الأطراف لا تركيزًا ثنائيًّا. ويبحث هذا القسم في التحديات والممارسات الجيدة بالقياس إلى التعاون الدولي من خلال نتيجتَيْن تشغيليتين: الأولى هي استرداد الأموال والثانية الإنفاذ والملاحقة الجنائية.

1-5 استرداد الأموال

85. إنّ أكبر تحدٍّ لاسترداد أموال الاحتيال الذي يسهّل الإنترنت ارتكابه هو سرعة وتيرة غسل الأموال. وللتخفيف من شدّة هذا التحدي، ظهرت برامج "استجابة سريعة" متعدّدة الأطراف أنشأتها هيئات مختلفة لتتبُّع متحصلات الاحتيال الذي يسهّل الإنترنت ارتكابه واستردادها، ومنها برنامج الإنتربول للوقف السريع العالمي للمدفوعات (I-GRIP)، ومشروع اختراق البريد الإلكتروني التجاري وهو مشروع تابع لمجموعة إيغمونت، والسلسلة المالية الأمريكية لإنهاء الاحتيال. وبالعموم، تُظهر الخبرة المكتسبة من هذه الهيئات أنّ التدخل يكون أكثر فعّالية خلال 24 إلى 72 ساعة من وقت وقوع المعاملة الاحتيالية. وهذه إنما هي ممارسات جيّدة تخفّف من مخاطر تبديد الأموال إلى طبقات تمويه لاحقة متعدّدة، وهذا التخفيف يؤدّي إلى تضييق نطاق التحقيق في جرائم غسل الأموال كثيرًا وتيسير استرداد المتحصلات غير المشروعة.

المربع 40: فريق سلسلة مكافحة الاحتيال المالي واسترداد الأصول

أنشأ مكتبُ التحقيقات الفيدرالي (FBI) وجهاز مكافحة الجرائم المالية (وهي وحدة الاستخبارات المالية الأمريكية) سنة 2016 سلسلةَ مكافحة الاحتيال المالي استجابةً لتزايد مخطّطات اختراق البريد الإلكتروني التجاري. وتحاول السلسلة الإعانة على استرداد التحويلات البرقية الدولية المرسلة وفقًا لمخططات الاحتيال، فتستفيد من علاقات التي بين جهاز مكافحة الجرائم المالية وبين مجموعة إيغمونت لوحدات الاستخبارات المالية. ولا يمكن تنفيذ هذا الاسترداد إلا إذا كان التحويل المصرفي الاحتيالي يستوفي المعايير التالية: (1) أن يكون التحويل بقيمة 50,000 دولار أمريكي أو أكثر، (2) وأن يكون التحويل دوليًّا، (3) وأن يكون إشعار استرجاع تحويل سويفت قد ابتدأ، (4) وأن يكون التحويل قد وقع خلال الـ72 ساعة الماضية.

وفي سنة 2018، أنشأ مركز شكاوى جرائم الإنترنت (IC3) التابع لمكتب التحقيقات الفيدرالي (FBI) فرقة استرداد الأموال (RAT) من أجل معالجة مواطن الضعف في التحويلات المصرفية المحلية. وتعمل فرقة استرداد الأموال على تسهيل الاتّصال بالمؤسسات المالية ويساعد المكاتب الميدانية لمكتب التحقيقات الفيدرالي في تجميد الأموال المخصّصة للتحويلات المحلية التي تقع بذرائع احتيالية. وقد حققت فرقة استرداد الأموال عددًا من النجاحات الملحوظة، إذ جمّدت 73% من الأموال التي أُبلِغ مركز شكاوى جرائم الإنترنت عن أنها احتيالية (433.3 مليون دولار أمريكي من أصل 590.62 مليون دولار أمريكي) حتى الآن. ووفقًا لمثال حالة الولايات المتحدة، يمكن لهذا البرنامج في بعض الحالات التعرّف بسرعة على حسابات التنقُّل الثاني وتجميد أموالها، وهذا إنما يجعل الاسترداد الكامل للأموال أمرًا ممكن الحدوث.

المصدر: الولايات المتحدة

86. إن أوّل ما تهدف إليه هذه البرامج المتعدّدة الأطراف هو القيام بأمرين: جمع الحدّ الأدنى من المعلومات المطلوبة لإجراءات إنفاذ القانون وإعطاء تلك المعلومات إلى "الأيدي الصحيحة". ولضمان الاستجابة الفعّالة عبر الحدود، تتّفق جميع عُقَد الشبكات المتعدّدة الأطراف أيضًا على قواعد الحوكمة وإجراءاتها. وصحيح أنّ هذه الشبكات المتعدّدة الأطراف عادةً ما تكون عالميّة بطبيعتها، ولكن قد تُفِيدُ المبادرات الإقليمية أيضًا في تخفيف التحديات، وذلك من خلال الاعتماد على التعاون الإقليمي القائم في الأصل.

المربع 41: مشروع مكافحة الاحتيال المتعدّد الولايات القضائية

نظرًا لطبيعة الاحتيال العابرة للحدود، وُضِعت مبادرةٌ إقليمية ضمن المجموعة الاستشارية للاستخبارات المالية[1] اسمها مشروع مكافحة الاحتيال المتعدّد الولايات القضائية. واشترك في قيادة هذه المبادرة وحدات الاستخبارات المالية في ماليزيا وإندونيسيا وسنغافورة، والغرض منها كشف الأموال وتتبُّع واستردادها من أجل للضحايا.

ثم أُنشِئت آلية استجابة تتضمن معاملات عابرة للحدود بين الدول الأعضاء في المجموعة الاستشارية للاستخبارات المالية. وهذا المشروع سيعين أعضاء هذه المجموعة على تبادل معلومات الاستخبارات المالية بسرعة وسهولة، ومن ثمّ دعم الإجراءات السريعة التي تتّخذها السلطات لمكافحة الاحتيال واسترداد الأموال المسروقة.

المصدر: ماليزيا

1 إن المجموعة الاستشارية للاستخبارات المالية هي هيئة إقليمية مكوّنة من وحدات الاستخبارات المالية من جنوب شرق آسيا ونيوزيلندا وأستراليا.

جمع المعلومات وتبادلها عبر الحدود: "جمع الحد الأدنى من المعلومات"

87. حيثما يعدُّ الاحتيال الذي يسهّل الإنترنت ارتكابه جريمةً خطيرة بموجب القانون المحلي، فإنه يلزم تجريمه وعدّه جرمًا أصليًّا لغسل الأموال، ذلك بموجب التوصية 3 من توصيات مجموعة العمل المالي. ويضاف إلى ذلك أنه على عكس ضروب الاحتيال التقليدية المرتكبة بين المعارف، حيث يصعب التمييز بين الاحتيال والمنازعات المدنية المحتملة بين الدائن والمدين، فإن قضايا الاحتيال الذي يسهّل الإنترنت ارتكابه يسهل نسبيًّا إثبات جرميّتها ظاهريًّا، إذ لا يكون الاحتيال فيها عادةً بين المعارف. وهذا يخفّف من الحاجة إلى استمرار طلب المساعدة في توضيح الصلة الإجرامية وتعريفها، كما يُطلَب عادةً في أنواع أخرى من الجرائم (التي لا يُعترَف بها عالميًّا على أنها جرمٌ أصليّ).

88. ومن الممارسات الجيّدة أن برامج الاستجابة السريعة المختلفة تستخدم نماذج لتسريع جمع المعلومات وتبادلها. إذ تتيح النماذج الجمعَ السريع للحدّ الأدنى من المعلومات المطلوبة لإثبات الجريمة. وهي تُعِين على تركيز جهود وحدات الاستجابة الميدانية على الأنواع الهامّة من الأدلة أو المعلومات التي يجب تحصيلها في المراحل الأولى من الشكوى الجنائية. وتخفّف هذه النماذج أيضًا من التحديات المتعلقة بجودة المعلومات المتبادلة، وتُحسّنُ استجابةَ أجهزة إنفاذ القانون عبر الحدود.

89. يضاف إلى إيراد النماذج لملخّص يصف جريمة الاحتيال الذي يسهّل الإنترنت ارتكابه، فإنها تسعى عمومًا إلى جلب البيانات الأساسية اللازمة من أجل تعزيز جهود المبذولة في تتبُّع الأموال. ثم إنّ التوحيد القياسيّ للطلبات يتيح للولايات القضائية المطلوبة أن تُعالِج كلَّ طلبٍ واردٍ معالجةً سريعة، وهذا يسرُّع قدرة إنفاذ القانون على اعتراض الأموال غير المشروعة التي دخلت إلى ولايتها القضائية.

90. قد تتضمن حقول البيانات في النماذج معلومات حساب المنشئ والمستفيد ومعلومات المعاملة (التاريخ والوقت والمبالغ المحوَّلة). ولتعزيز الفعّالية أكثر فأكثر، يمكن أن تتضمّن النماذج أيضًا معلومات حول الوجهة التالية للأموال إذا حُوّلت الأموال بالفعل من حساب المستفيد. وقد يكون من المفيد أيضًا تقليل كل قيد مفروض على الولايات القضائية لنشر أي معلومات تتبادلها مع السلطات المختصّة المعنيّة محليًّا عند استلامها.

المربع 42: آلية الإنتربول لوقف المدفوعات (I-GRIP)

أنشأ الإنتربول نظام الإنتربول للوقف السريع العالمي للمدفوعات (I-GRIP)، وهو عبارة عن آلية عالمية لوقف الدفع تُمكّن البلدان الأعضاء من تقديم ومعالجة طلبات تتبُّع المتحصلات غير المشروعة للاحتيال الذي يسهّل الإنترنت أو اعتراضها أو تجميدها مؤقّتًا. والآلية معروفة باسم I-GRIP، ولكنها حين جُرّبت في أول أمرها كان اسمها بروتوكول الاستجابة السريعة لمكافحة غسل الأموال (ARRP) في سنة 2022، ثم أُطلِقت رسميًّا في نوفمبر/تشرين الثاني 2022 بفضل كثيرٍ من حالات نجح فيها إيقاف الدفع خلال المرحلة التجريبية.

وتعمل آلية I-GRIP على تيسير الاتّصال السريع بين مكاتب الإنتربول المركزية الوطنية من أجل منع نقل الأصول غير المشروعة المشتبه فيها بين البلدان الأعضاء. ويجب أن تتضمّن الطلبات المقدمة عبر آلية وقف المدفوعات I-GRIP تفاصيل كافية يمكن لمكتب الإنتربول المركزي الوطني المتلقّي التصرف بناءً عليها، ومثال ذلك: تاريخ المعاملة والعملة والمبلغ وأرقام الحسابات وأسماء المؤسسات المالية لحسابات المستفيدين والمرسلين.

المصدر: الإنتربول

91. يُضاف إلى ذلك أنّ حقول البيانات الموحدة قياسيًّا في النماذج تمكّن المنظمات الدولية ذات القدرات المركزية من تحليل البيانات بسهولة وتحقيق أكبر قدر من الجهد المبذول في التحقيق واسترداد الأموال. ومثال ذلك أنّ الإنتربول يستفيد من المعلومات المتبادلة عبر قنواته لإنشاء قاعدة بيانات داخلية، وهي ملف تحليل الجرائم المالية (FINCAF)، والغرض منها تيسير تحليل المعلومات الاستخبارية العابرة للحدود الوطنية عن مختلف ضروب الجرائم المالية، وتحديد الروابط بين ما هو عابرٌ للحدود من قضايا وتحقيقات وتهديدات واتجاهات الجريمة وشبكات إجرامية (انظر المربع 45 أدناه).

92. ومن أجل تسريع إجراءات استرداد الأموال أكثر، مكّنت بعض الولايات القضائية الضحايا الأجانب من تقديم شكوى بشأن الاحتيال الذي يسهّل الإنترنت ارتكابه مباشرةً إلى وكالات إنفاذ القانون التابعة لبلادهم، ومما أتاح ذلك منصةٌ للإبلاغ عبر الإنترنت خاصة بهم تلتقط حقول البيانات المطلوبة مباشرةً لإجراءات الإنفاذ (انظر القسم الخاص ببلاغات الضحايا أعلاه). وهذا يزيل مرحلة إضافية من الاتّصالات ويسمح للسلطات المختصة باتّخاذ كل تدبير متاح سريعًا ضد المعاملات المشبوهة التي تجري على حسابات المستفيدين في ولاياتها القضائية.

الصلاحيات الضرورية للتصرُّف: "الأيدي الصحيحة"

93. إنّ السرعة أمرٌ جوهري، لذلك فمن الأفضل أن تُسلّم أي معلومات تُجمَع مباشرةً إلى السلطات المُجهَّزة أصلاً بالصلاحية والخبرة المناسبتين لتتبُّع الأموال واستردادها. ويتيح ذلك اتّخاذ تدابير مؤقتة فورَ تلقّي طلبٍ لمنع مزيد من غسل الأموال أو تبديدها. وهذا يعطي سلطات إنفاذ القانون وقتًا بالغ الأهمية تحتاج إليه لمواصلة تحقيقاتها وجمع الأدلة وإعدادها ومتابعة الطلبات الرسمية للمساعدة القانونية المتبادلة.

المربع 43: طلب تأجيل من كيان ملزَم

تلقّت وحدة الاستخبارات المالية في إيطاليا طلب تأجيل من أحد الكيانات الملزَمة بشأن أربع تحويلات مصرفية مشبوهة تصل قيمتها إلى 490 ألف يورو. وقد طلبت إجراءَ هذه المعاملات شركةٌ إيطالية لتجارة الملابس بالجملة لصالح شركات مختلفة في إحدى دول شرق آسيا.

رأى الكيان الملزَم المعاملات الأربع مشبوهةً لأن أصل الأموال من تحويلات واردة استرجعَها البنك الطالب على أساس أن الأموال أُرسِلت بسبب "احتيال رئيسٍ تنفيذيّ" من شركة ضحية في أوروبا الغربية. فتلقت وحدة الاستخبارات المالية في إيطاليا أيضًا تبادلًا دوليًا من غير سابق معرفة للمعلومات من وحدة الاستخبارات المالية في الدولة المذكورة الواقعة في أوروبا الغربية. وأبلغت وحدة الاستخبارات المالية أيضًا بأن الشركة الإيطالية يحتمل ارتباطها بمخططاتِ احتيال على ضريبة القيمة المضافة اشتركت فيه الدولة الآسيوية المذكورة من خلال دولة منفصلة في أوروبا الشرقية، وهو ما قدَّم مؤشرًا إضافيًا على الروابط بين الاحتيال الذي يسهّل الإنترنت ارتكابه وأنواع أخرى من الجريمة المنظّمة.

فأُجّلت المعاملات بنجاح. فسمح ذلك للسلطات الأجنبية بإصدار أمر مصادرة أجنبي لاسترداد الأموال في إيطاليا.

المصدر: إيطاليا

94. لكن قد يواجه هذا التواصل المباشر تحديات بسبب اختلاف الأطر التشريعية وأطر الإنفاذ عبر الولايات القضائية. ومن الممارسات الجيّدة للتخفيف من هذه التحديات إنشاءُ آليات تنسيق محلية لتيسير تحويل الطلبات إلى السلطات الصحيحة، والاستفادةُ من قنوات التعاون بين القطاعين العام والخاص وقدرة المؤسسات المالية على اتخاذ تدابير احتياطية طوعية بمجرد أن تُبلِغها السلطات المختصة بالمعاملات المشبوهة.

الحوكمة والقواعد: "الاتفاقية الجماعية"

95. تتيح الحوكمة والقواعد الخاصة بالأُطُر المتعدّدة الأطراف ضماناتٍ والتزامًا بالاعتراف المتبادل بالنشاط الإجرامي وبالتصرف سريعًا عند تلقّي المعلومات. ويساعد ذلك في التغلُّب على التحدي المتمثّل بعدم اتفاق الأولويات بين الوكالات الدولية، ففي الحوكمة والقواعد اتفاق مسبق على شروط الانضمام وتقديم المساعدة. ومن الممارسات الجيّدة في هذا الشأن أنه يجب أن تكون تلك القواعد والمعايير واضحةً وسهلةَ الفهم.

96. وتنطبق المبادئ المذكورة أعلاه على آليات التعاون الدولي غير الرسمية، وكذلك على آليات التعاون الدولي الرسمية. والأمثلة الجيّدة لذلك أنّ لائحة الاتحاد الأوروبي ذات الرقم 1805/2018 الصادرة عن البرلمان الأوروبي ومجلس أوروبا تسمح بالاعتراف المتبادل بالأوامر الأجنبية في التجميد والمصادرة. كما تتيح آلية التَّنفيذ المباشر هذه بالتدخل السريع عبر الحدود.

97. لا ينبغي أن يكون ثمن تبادل المعلومات المُعجَّل إهمال حماية البيانات وسرّيتها. ولضمان أمن المعلومات المنقولة، تستفيد الأُطُر المتعدِّدة الأطراف عادةً من قنوات الاتصال الآمنة الموجودة أصلاً، مثل القنوات التي يتيحها الإنتربول واليوروبول ومجموعة إيغمونت. كما تُمكّن قنوات الاتصال الآمنة الحالية هذه الأُطُرَ المتعدِّدةَ الأطراف من التوسع بسهولة، لأنها تتجاوز الحاجة إلى تطوير قنوات اتّصال ثنائية.

المربع 44: فريق مشروع إيغمونت لاختراق البريد الإلكتروني التجاري

أطلقت 11 وحدة استخبارات مالية فريق مشروع إيغمونت لاختراق البريد الإلكتروني التجاري (Egmont BEC Project Team)، وذلك لمعالجة التهديد المتزايد والخطير الذي يمثّله هذا الاختراق على المؤسسات المالية وعملائها، وركّز المشروع على تحليل اتجاهات اختراق البريد الإلكتروني التجاري ومؤشراته ومنهجياته، إضافةً إلى مشاركة النتائج الرئيسية مع وحدات الاستخبارات المالية. وقد أظهرت التطبيقات المالية ودراسات الحالة المشتركة لاختراق البريد الإلكتروني التجاري أن رد الفعل السريع لإيقاف التحويلات البرقية وتتبُّعها هو أكثر الطرق فعاليةً للتصدّي لهذا النوع من الجرائم.

ولهذا وضع فريق المشروع[1] بروتوكولات بين سلطات إنفاذ القانون ووحدات الاستخبارات المالية، وبين وحدات الاستخبارات المالية الدولية لتتبُّع متحصلات اختراق البريد الإلكتروني التجاري وتجميدها.

- عند استلام تقرير المعاملات المشبوهة المتعلق بتدفقاتٍ مالية مشتبه في أنها آتية من اختراق البريد الإلكتروني عبر الحدود، تُعِدُّ وحدة الاستخبارات المالية التي في المصدر طلبَ "استجابةٍ سريعة" إلى وحدة الاستخبارات المالية التي في الوجهة.
- يجب أن يحتوي الطلب على البيانات والمعلومات الأساسية المتّفق عليها والمطلوب تبادلها لإجراءات التنفيذ.
- يُطلَب من وحدة الاستخبارات المالية التي في الوجهة اتّخاذ إجراءاتٍ فورية (حيثما أمكن) لتعليق المتحصلات غير المشروعة واستردادها، ويُفضَّل أن يكون ذلك في خلال 72 ساعة من وقت وقوع الجريمة.

ويستفيد مشروع اختراق البريد الإلكتروني التجاري من منصة الاتصالات الآمنة التي خصّصها مجموعة إيغمونت لتبادل طلبات "الاستجابة السريعة".

المصدر: مجموعة إيغمونت

1 يتألّف أعضاء فريق المشروع حاليًا من: وحدة الاستخبارات المالية الأسترالية (AUSTRAC) (أستراليا)، ووحدة الاستخبارات المالية البنغلاديشية (BFIU)، ووحدة الاستخبارات المالية البلجيكية (CTIF-CFI)، ووحدة الاستخبارات المالية الفرنسية (TRACFIN)، ووحدة الاستخبارات المالية في غانا (GHFIU)، ووحدة الاستخبارات المالية الهنغارية (HFIU)، ووحدة الاستخبارات المالية الإسرائيلية (IMPA)، ووحدة الاستخبارات المالية اللبنانية (SIC)، ووحدة الاستخبارات المالية في لوكسمبورغ، ووحدة الاستخبارات المالية الماليزية (UPWBNM)، وجهاز مكافحة الجرائم المالية في الولايات المتحدة الأمريكية (FinCEN)، واليوروبول.

2-5 إنفاذ القانون والملاحقة الجنائية

98. إلى جانب الصعوبات في استرداد الاموال، أدّت الطبيعة العابرة للحدود الوطنية للاحتيال الذي يسهّل الإنترنت ارتكابه أيضًا إلى صعوبات في جميع مراحل عملية الإنفاذ، ابتداءً من جمع المعلومات الاستخبارية والتحقيق حتّى جمع الأدلة من أجل الملاحقة الجنائية. فقد أدى تطوُّر التكنولوجيا إلى تسريع المعاملات وتيسير العمليات المجزّأة عبر الحدود، كما أنه زاد الوقت والجهد اللازمين لإنفاذ القانون من أجل تتبُّعها وتحديدها.

جمع الأدلة الرقمية

99. على الرغم من أنّ الأدلة الجنائية الرقمية غير محصورٍ تعلُّقها بغسل الأموال، إلا أنها يمكن أن تكون أدلةً مهمةً لتوجيه جهات إنفاذ القانون إلى تعزيز تحقيقاتها في جرائم غسل الأموال. ثم إن توافر خدمات إخفاء الهوية وسهولة استخدامها على نطاق واسع، كالشبكة الخاصة الافتراضية، يزيد العراقيل أمام الجهود المبذولة في تحديد المرتكبين النهائيين للاحتيال الذي يسهّل الإنترنت ارتكابه.

100. وللأسف لا يوجد اليومَ نظامٌ عالميٌّ واحد يحكم مدة الاحتفاظ بالبيانات الرقمية، ومنها البيانات المتعلقة بمزوّدي الخدمات التقنية. وسلطت كثير من الولايات القضائية الضوءَ على المخاطر الكبيرة المتمثلة في تبديد الأدلة الرقمية. كما أن التأخير في آليات التعاون الرسمية من شأنه أن يشكل تحديًا في جلب الأدلة الرقمية بسرعة.

101. على أنه هناك كثير من الممارسات الجيّدة التي يمكن أن يُخفَّفَ بها من شِدّة هذه التحديات.

- **الاستفادة من القنوات غير الرسمية** أولَ شيءٍ لجمع المعلومات الاستخبارية وتأمينها. ثم تُستخدَم بعد ذلك قنوات التعاون الرسمية للحصول على الأدلة والبيانات الضرورية لإعداد الإجراءات القضائية.
- **الاتفاقيات وأدوات التحقيق** مثل اتفاقية الجرائم الإلكترونية (Convention on Cybercrime)، المعروفة أيضًا باسم اتفاقية بودابست، فهي تسمح بالحفظ السريع للبيانات الإلكترونية ونقل المعلومات دون طلب مسبق، وهذا يُعِين على تعجيل تحديد هوية المرتكبين النهائيين للاحتيال الذي يسهّل الإنترنت ارتكابه. وتنصُّ اتفاقية بودابست أيضًا على إنشاء شبكةٍ تعمل على مدار الساعة طوال أيام الأسبوع لضمان المساعدة الفورية في التحقيق كتقديم المشورة الفنية وجمع الأدلة والحفاظ على البيانات وما إلى ذلك.
- **التعاون المباشر** مع مزوّدي الخدمات الأجانب للحصول على الأدلة الجنائية الضرورية، كمعلومات المُشترِك من غير الدخول في المساعدة القانونية المتبادلة. وذكرت إحدى الولايات القضائية أنّ التعاون الطوعي المباشر من مزوّد الخدمة الأجنبية هو أكثر الآليّات فعاليةً في جمع الأدلة الرقمية المناسبة.[22]

المربع 45: اتفاقية بودابست

نصّت اتفاقية بودابست على سلطات إجرائية من أجل: الحفظ السريع للبيانات المخزّنة، والحفظ السريع والكشف الجزئي عن بيانات حركة المرور، وعن أمر الإصدار، والبحث عن بيانات الحاسوب ومصادرتها، وجمع بيانات حركة المرور الآنية، واعتراض بيانات المحتوى. وهذه الاتفاقية أتاحت أيضًا نظامًا سريعًا وفعّالًا للتعاون الدولي.

ثم إنّ البروتوكول الإضافي الثاني لاتفاقية الجرائم الإلكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية يتيح أساسًا قانونيًا للكشف عن معلومات تسجيل أسماء النطاقات، وللتعاون المباشر مع مزوّدي الخدمات للحصول على معلومات المشتركين، ويتيح أيضًا وسائل فعّالة للحصول على معلومات المشتركين وبيانات حركة المرور، وللتعاون الفوري في حالات الطوارئ، ولتوفير أدوات للمساعدة المتبادلة، إضافةً إلى توفير ضماناتٍ لحماية البيانات الشخصية.

المصدر: مجلس أوروبا

إجراءات الإنفاذ المشتركة

102. إن لفِرَق التحقيق المشترك عبر الحدود اتفاقًا قانونيًا بين السلطات المختصة في ولايتين قضائيتين أو أكثر بغرض إجراء التحقيقات الجنائية. وقد يُيَسِّر ذلك تبادلَ المعلومات وتتبُّع الأموال عبر الحدود. وعادةً ما يُعزِّز تبادلُ المعلومات بأُطُر واتفاقيات مختلفة (منها مثلاً، يوروجست، وفرقة العمل المشتركة المعنية بالجرائم الإلكترونية، ويدعم هذه الفرقة اليوروبول).

103. وتتيح فِرَق التحقيق المشترك أيضًا نقطة تنسيق مهمة لإجراءات الإنفاذ المتعددة الأطراف ضد الاحتيال الذي يسهّل الإنترنت ارتكابه، وذلك نظرًا لعملياتها غير المركزية والعابرة للحدود الوطنية. ومع انخفاض المعوقات أمام العمليات الإجرامية، أمكن لعصابات الاحتيال الذي يسهّل الإنترنت ارتكابه الانتقال بسهولةٍ وإنشاء مراكز رقمية جديدة يجرون بها عملياتهم عن بُعد. ومن ثمّ، فإن التنسيق ضروريٌّ لاقتلاع الجماعات الفرعية المختلفة (التي يمكن أن تعمل عبر ولايات قضائية متعدّدة) في آنٍ معًا.

22 لمزيد من المعلومات حول التعاون الطوعي مع مزوّدي الخدمات الأجانب، انظر مجلس أوروبا (يوليو/تموز 2020) اتفاقية بودابست المتعلقة بالجريمة الإلكترونية: الفوائد والأثر في الممارسة العملية.

المربع 46: العمل المشترك ضد الاحتيال الاستثماري على نطاق واسع[1]

شاركت صربيا، مع النمسا وبلغاريا وألمانيا، وبدعمٍ من يوروجست، في عمليات ناجحة ضد جماعتَيْن من جماعات الجريمة المنظمة يشتبه في ارتكابهما عمليات احتيال بالاستثمار واسعة النطاق في التجارة عبر الإنترنت. وألقت السلطات الصربية القبض على خمسة من المشتبه بهم وفتشت تسعة مواقع، وصادرت خمس شقق وثلاث سيارات وكَمًّا كبيرًا من النقود ومعدات تكنولوجيا المعلومات. كما وضع أكثر من 30 حسابًا مصرفيًا صربيًا تحت المراقبة. ويضاف إلى ذلك أنه اعتُقل أربعةٌ من المشتبه بهم في بلغاريا، وجُمِّد مبلغ 2.5 مليون يورو في الحساب المصرفي لشركة متورطة في مخطط الاحتيال في ألمانيا.

واستنادًا إلى معلومات جُمِعَت في العملية، انخرطت السلطات سريعًا في عملية أخرى ضد شركة في بلغراد بعد يومين، واعتقلت أحد المشتبه بهم وصادرت الخوادم ومعدات تكنولوجيا المعلومات الأخرى ووثائق.

وفي هذه الحالة، استخدمت السلطات الصربية، في جملة من الأمور، المادة 26 من اتفاقية بودابست (قسم المعلومات التي دون طلب مسبق) لكي تتبادل المعلومات مع شركاء آخرين. وأعانت يوروجست أيضًا على التحقيقات من خلال تمويل فرقة تحقيق مشترك، وتنظيم اجتماع تنسيقيّ في مقرها في لاهاي وعقد مؤتمر عبر الفيديو.

المصدر: صربيا، ومجلس أوروبا (يوليو 2020) اتفاقية بودابست بشأن الجرائم الإلكترونية: الفوائد والأثر في الممارسة العملية

1 لمزيد من المعلومات، انظر البيان الصحفي ليوروجست (أبريل/نيسان 2020) المتاح على هذا الرابط: www.eurojust.europa.eu/news/action-against-large-scale-investment-fraud-several-countries

104. ومع ذلك، هناك أيضًا تحدّيات مرتبطة بإجراءات الإنفاذ المشتركة.

- فقد تؤدي **المعوقات القانونية** إلى تقييد تبادل المعلومات غير الرسمي حتى داخل فِرَق التحقيق المشترك. وأعربت إحدى الولايات القضائية عن ضرورة الاستمرار في الاعتماد على طلبات المساعدة القانونية المتبادلة للسماح بتبادل المعلومات، وهذا قد يعيق الفعّالية والمشاركة. وربما كانت هناك أيضًا قيودٌ للمعلومات التي يمكن مشاركتها، ولا سيّما فيما يتعلق بدقّة معلومات المعاملات المالية.
- وقد تؤدي **القدرات والأولويات غير المتكافئة** أيضًا إلى تَثْني الولايات القضائية عن الإسهام في العمل المشترك. وكما ناقشنا سابقًا، فربما لا تتمشّى الأولويات المحلية الداخلية مع العمل المشترك وقد تواجه الولايات القضائية اتّخاذ قرار صعب في موازنة هذه المصالح من أجل مواجهة قيود الموارد على الرغم من ازدياد الاحتيال الذي يسهّل الإنترنت ارتكابه.

105. وإضافةً إلى فِرَق التحقيق المشترك، توفر العمليات المشتركة التي تنظّمها منظمات متعدّدة الأطراف كالإنتربول نقطةَ تنسيق مهمة لإجراءات الإنفاذ المتعدد الأطراف ضد الاحتيال الذي يسهّل الإنترنت ارتكابه. وفي حين أن هذه العمليات قد تكون غير رسمية أكثر من كون فِرَق التحقيق المشترك غير سمية في ظل غياب الاتفاقيات القانونية الرسمية، ما تزال هذه العمليات قادرةً على إتاحة منصةٍ مهمة للسلطات القضائية ذات الصلة لمحاربة الاحتيال الذي يسهّل الإنترنت ارتكابه محاربةً مشتركة.

المربع 47: عملية الإنتربول المسمّاة هايتشي (HAECHI)

لم يزل الإنتربول منذ سنة 2020 ينفذ عملية سنوية تسمى هايتشي (HAECHI) تستهدف الجرائم المالية التي يسهّل الإنترنت ارتكابها وغسل الأموال المتصل بها، وتدعم تبادل المعلومات بين الولايات القضائية المشاركة. وبموجب عملية هايتشي 3 الأخيرة (في سنة2022)، التي شاركت فيها 30 ولاية قضائية، اعتُقل زُهاء 1000 مشتبه به وحُظِر 2800 حساب مصرفي وحسابات أصول افتراضية مرتبطة بمتحصلات غير مشروعة بلغت 130 مليون دولار أمريكي. ومن خلال عملية هايتشي 3 نسّق الإنتربول كثيرًا من القضايا بين البلدان الأعضاء لمكافحة الاحتيال الذي يسهّل الإنترنت ارتكابه مكافحةً مشتركة.

واستُخدِمت عملية هايتشي أيضًا كمنصة لملف تحليل الجرائم المالية للذي يجمع المعلومات من مصادر شتّى ويحدّد الروابط بين التحقيقات الجارية في مختلف البلدان الأعضاء. وقد صُمِّم ملف تحليل الجرائم المالية ليشمل البيانات وغيرها من عناصر المعلومات المتعلقة بأي نوع من أنواع الجرائم المالية والجرائم ذات الطبيعة العابرة للحدود الوطنية. ويستخدم الإنتربول ملفَّ تحليل الجرائم المالية للعمل مع البلدان الأعضاء على تعزيز الاستجابة التكتيكية الشاملة للجريمة المنظمة الدولية كالاحتيال الذي يسهّل الإنترنت ارتكابه. ويعدُّ ملفُ تحليل الجرائم المالية أداةً مهمّةً تتيح أفكارًا مستنيرةً حول الأنشطة الإجرامية عبر الحدود، والمنظمات الإجرامية، وبنية جماعاتها، وأدوارها الفردية وأشخاصها البارزين، وطرق عملها، ومعاملاتها المالية الاحتيالية.

المصدر: الإنتربول

التعاون بين القطاعَيْن العام والخاص

106. يمكن أن يمتدَّ التعاون بين القطاعَيْن العام والخاص إلى ما هو أبعد من الحدود الوطنية، وهذا يحقّق نتائج أكبر نظرًا لامتداد الاحتيال الذي يسهّل الإنترنت ارتكابه امتدادًا عابرًا للحدود الوطنية. وكما هو الحال مع الشراكات المحلية بين القطاعَيْن العام والخاص، يمكن أن يستوعب هذا التعاون التطبيقات أو التبادل الإستراتيجي للمعلومات، إضافةً إلى تنسيق العمليات. ويعتمد تكوين هذه الشراكات أيضًا على الأهداف، وقد يشمل القطاعات التقليدية ذات الصلة بمكافحة غسل الأموال وتمويل الإرهاب والقطاعات غير التقليدية.

المربع 48: عملية بغل المال الأوروبية

إن عملية بغل المال الأوروبية هي عملية دولية مبنية على تبادل المعلومات بين القطاعَيْن العام والخاص لمحاربة الجرائم الحديثة المعقّدة.

وفي سنة 2022، دعم نحو 1800 بنك ومؤسسة مالية إنفاذ القانون في هذه العملية، وذلك بالتنسيق المستمر مع الاتحاد المصرفي الأوروبي، ودعمت إنفاذه أيضًا في خدمات تحويل الأموال عبر الإنترنت، ومنصات تبادل العملات الرقمية، وشركات التكنولوجيا المالية وشركات تقنية اعرف عميلك، وشركات تكنولوجيا الحاسوب المتعدّدة الجنسيات.

وتألّفت العملية من سلطاتٍ لإنفاذ القانون من 25 ولاية قضائية[1]، ونالت دعمًا إضافيًّا من اليوروبول، ويوروجست، والإنتربول. ومن نتائجها أنها حدَّدت 8,755 من بغال المال إلى جانب 222 من مُعيّني بغال المال ومستخدميهم. وبالجملة، اعترضت من الأموال 17.5 مليون يورو، واعتقلت 2469 من بغال المال.

المصدر: اليوروبول

1 أستراليا، والنمسا، وبلغاريا، وكولومبيا، وقبرص، وجمهورية التشيك، وإستونيا، واليونان، والمجر، وسنغافورة، وهونج كونج (الصين)، وأيرلندا، وإيطاليا، ومولدوفا، وهولندا، وبولندا، والبرتغال، ورومانيا، وجمهورية سلوفاكيا، وسلوفينيا، والسويد، وسويسرا، وإسبانيا والمملكة المتحدة والولايات المتحدة.

6 الاستنتاج والمجالات ذوات الأولوية

107. الاحتيال الذي يسهّل الإنترنت ارتكابه جريمة ترتكبها عصابات جريمة منظّمة عابرة للحدود الوطنية. ومن المتوقع أن يكثر الاحتيال الذي يسهّل الإنترنت ارتكابه وتتّسع رقعته مع الاتجاه المتزايد للرقمنة والخدمات الافتراضية في جميع أنحاء العالم. فيجب أن تكون الولايات القضائية أيضًا على دراية بمواطن الضعف الإضافية في شتّى القطاعات، ومنها المؤسسات المالية الرقمية والقطاعات غير التقليدية، فهي التي قد يستغلها المجرمون لتعزيز تقنيات الاحتيال الذي يسهّل الإنترنت ارتكابه وغسل الأموال من خلال الرقمنة المتنامية.

108. يتعيّن على الولايات القضائية أن تركز على كسر العزلة لتسريع وتعزيز التعاون بين مختلف القطاعات والكيانات، على المستويين المحلي والدولي. فنظرًا للطبيعة غير المركزية للاحتيال الذي يسهّل الإنترنت ارتكابه وما يتّصل به من غسل الأموال، كثيرًا ما تكون المعلومات والأدلة المالية العامّة مجزّأةً في مواقع مختلفة. وهذا يؤدي إلى عرقلة الجهود المبذولة للتحقيق في عصابات الاحتيال الذي يسهّل الإنترنت ارتكابه وتفكيكها، وتتبُّع متحصلات هذا الاحتيال واستردادها.

109. يمكن أن يكون للاحتيال الذي يسهّل الإنترنت ارتكابه تأثيرٌ مالي شديدٌ على الضحايا ومعوّق لهم. ولكن هذا التأثير لا يقتصر على الخسائر المالية، بل يمكن أن يمتدَّ ليكون له آثار اجتماعية واقتصادية مُدمِّرة. وتشير استنتاجات هذا التقرير إلى ثلاثة مجالات ذوات أولوية ينبغي للولايات القضائية أن تعمل من أجلها للتصدِّي للاحتيال الذي يسهّل الإنترنت ارتكابه وما يتّصل به من غسل الأموال بشكل أكثر فعّالية: تعزيز التنسيق الداخلي، ودعم التعاون المتعدّد الأطراف، وتعزيز الكشف والوقاية.

المجالات ذوات الأولوية لمكافحة الاحتيال الذي يسهّل الإنترنت ارتكابه وما يتّصل به من غسل الأموال مكافحةً فعّالة

تعزيز التنسيق الداخلي بين القطاعَيْن العام والخاص

- ينبغي على الولايات القضائية وضع آليّات تنسيق لجمع السلطات المختصة المعنية للتصدّي للاحتيال الذي يسهّل الإنترنت ارتكابه وغسل المتحصلات المتصلة به بصورة شاملة. ويتضمّن ذلك خبراء الجرائم الإلكترونية التقنيّين، ويضاف إليهم القطاعات غير التقليدية مثل منصات التواصل الاجتماعي والتجارة الإلكترونية ومزوّدي خدمات الاتصالات والإنترنت. ويجب على الولايات القضائية أيضًا الاستفادة من الشراكات بين القطاعَيْن العام والخاص لتحسين الكشف والتحقيقات، وتسريع الاستجابات التشغيلية لاسترداد الأموال.
- ومن الممارسات الجيّدة إنشاء وحدة مركزية مخصّصة يمكنها الربط بين المعلومات ذات الصلة وتنسيق الإجراءات عبر مختلف القطاعات العامة والخاصة، ومن ذلك التحقيقات واسترداد الأموال والوقاية من الاحتيال.

دعم التعاون الدولي المتعدِّد الأطراف

- لتعزيز نتائج استرداد الأموال وتجنُّب تبديد المتحصلات المتّصلة بالاحتيال الذي يسهّل الإنترنت ارتكابه، يجب على الولايات القضائية أن تعمل معًا لاعتراض متحصلات هذا الاحتيال بسرعة. وتُظهِر الخبرة المستمدة من العمليات أن التدخُّل يكون أكثر فعّاليةً على العموم في خلال 24 إلى 72 ساعة من وقت وقوع الاحتيال الذي يسهّل الإنترنت ارتكابه. ويلزم اتباع نهج عالميّ موحد لتتبُّع متحصلات هذا الاحتيال واستردادها على نحوٍ فعّال، فهذه المتحصلات تُغسَل وتوزيعها عبر ولايات قضائية متعدّدة.
- ومن أجل تحقيق هذه الغاية، ينبغي للولايات القضائية أن تعمل على تعزيز الآليات المتعدّدة الأطراف الموجودة (وأيّ آلية مستقبلية أيضًا) ودعمها (كآلية I-GRIP التابعة للإنتربول ومشروع مجموعة إيغمونت المعني باختراق البريد الإلكتروني التجاري)، وذلك لتسريع التعاون الدولي وتبادل المعلومات لمكافحة الاحتيال الذي يسهّل الإنترنت ارتكابه. إذ تسمح هذه الآليات المتعدّدة الأطراف أيضًا للولايات القضائية بالتعاون والتفكيك الجماعي لعصابات هذا الاحتيال العابرة للحدود الوطنية.

تعزيز الكشف والوقاية

- ينبغي للولايات القضائية من أجل أن تُعزّز الكشف أن تضمن سهولة بلاغات الضحايا، ومثال ذلك أن تضمن ذلك من خلال منصّات مخصصة تسمح بالإبلاغ المُيَسَّر. ويجب على الولايات القضائية أيضًا أن تعمل مع القطاع الخاص على تحسين الإبلاغ عن المعاملات المشبوهة.
- ينبغي للولايات القضائية تعزيز الوعي والتنبّه ضد الاحتيال الذي يسهّل الإنترنت ارتكابه من خلال التثقيف العام، ومن ذلك تبادلُ العلامات المُنذِرة بهذا الاحتيال وتعزيز محو الأمية الإلكترونية. وللوقاية شأنٌ كبير في تقليل الربح الإجمالي لعصابات الاحتيال الذي يسهّل الإنترنت ارتكابه. فيمكن للولايات القضائية أيضًا أن تتعاون مع القطاع الخاص لدعم إستراتيجيات الوقاية من هذا الاحتيال، كإستراتيجية حماية المستهلك وإزالة الأدوات الإجرامية.

الملحق أ: مؤشرات مخاطر الاحتيال الذي يسهّل الإنترنت ارتكابه

إن مؤشرات المخاطر المحتملة الآتية مستمدةٌ من الخبرات والبيانات الواردة من الولايات القضائية عبر الشبكة العالمية لمجموعة العمل المالي ومجموعة إيغمونت والقطاع الخاص. وتهدف هذه المؤشرات إلى تعزيز الكشف عن المعاملات المشبوهة المتعلقة بالاحتيال الذي يسهّل الإنترنت ارتكابه. والقائمة مصنّفة بحسب جوانب مختلفة، ابتداءً من فتح الحساب إلى رصد المعاملات. ويمكن أن تكون المؤشرات متّصلة بالكيانات الخاضعة للتنظيم، ومنها المؤسسات المالية، ومزوّدو خدمات الأصول الافتراضية، والأعمال أو المهن غير المالية المحددة، وغيرها من المؤسسات المالية ومؤسسات الدفع.

وإن وجود مؤشر واحد متعلّقٍ بعميل أو معاملة قد لا يضمن وحده الاشتباه في جرم الاحتيال الذي يسهّل الإنترنت ارتكابه، كما أن مؤشرًا واحدًا لا يدلّ بالضرورة دلالةً واضحةً على مثل هذا النشاط. ولكنه يمكن أن يقود إلى مزيدٍ من الرصد والفحص على حسب الاقتضاء.

أنماط المعاملات

- معاملات سريعة أو فورية، ذات مبالغ عالية أو منخفضة بعد فتح الحساب، لا تتّفق مع غرض الحساب
- عمليات سحبٍ نقديّ أو تحويلات نقدية سريعة أو فورية لمبالغ كبيرة بعد استلام حوالة مالية بهدف إفراغ الحساب
- معاملات متكررة وكبيرة، لا تتّفق مع الملف الاقتصادي لصاحب الحساب (ومثال ذلك: التحويلات الدولية المفاجئة، أو عمليات سحب الأموال النقدية التي تجري ببطاقات الدفع في أجهزة الصراف الآلي الأجنبية، أو المشتريات الكبيرة من الأصول الافتراضية أو البضائع التي ستُصدّر إلى الخارج، أو الدفعات لصالح شركات أجنبية غير مرخصة إلى خدمات تحويل القيمة المالية)
- تحويلات أموال من وإلى الولايات القضائية ذات المخاطر العالية من حيث غسل الأموال
- معاملات كبيرة متكررة مع الشركات المنشأة حديثاً و/أو التي لا تتوافق أنشطتها الرئيسية مع الأنشطة التي يقوم بها المستفيد أو لها غرض عام
- دفعة صغيرة للمستفيد، بمجرد إتمامها بنجاح تتبعُها بسرعة دفعات ذات قيمة أكبر لنفس المستفيد
- عمليات شراء ذات قيمة صحيحة بلا فواصل عشرية متكررة و/أو مبالغها كبيرة، ويمكن أن تشير إلى شراء بطاقة الهدايا

تعليمات وملاحظات معاملات العملاء

- طلب معاملة لعميل من أجل إصدار دفعات إضافية مباشرةً بعد نجاح الدفع لحساب لم يستخدمه العميل سابقًا للدفع للموردين أو البائعين. فقد يتوافق هذا السلوك مع محاولة المجرم إصدارَ دفعاتٍ إضافية غير مصرّح بها عند علمه بنجاح الدفع الاحتيالي
- تعليمات لمعاملة عميلٍ تبدو مشروعةً تحتوي على لغة عامية مختلفة وتوقيت مختلف ومبالغ مختلفة عن تعليمات المعاملة التي تم التحقق منها سابقًا.
- تعليمات لمعاملة تحوي علامات أو تأكيدات أو لغة تحدّد طلب المعاملة على أنه "عاجل" أو "سري" أو "طي الكتمان"
- تقديم العميل رسائل أو رسائل بريد إلكتروني سيئة التنسيق (بأخطاء إملائية أو نحوية أو كليهما) كمسوّغ للمعاملة.
- تعليمات إجراء معاملة دفع مباشر إلى مستفيد معروف، ولكن معلومات حساب المستفيد تختلف عمّا استُخدِم سابقًا
- المستفيد المقصود في وصف المعاملة واسم صاحب الحساب المعروف لدى البنك المستفيد غير متطابقين
- تحويلات يطلبها أشخاص طبيعيون (مستثمرون مزعومون) ليس لديهم خبرة مالية ولا تجربة، لصالح الشركات (في كثير من الحالات المنشأة في ولايات قضائية عالية المخاطر) لأسباب تتعلق بدفعات غرضها استثمارات ومنتجات مالية

- أطراف لا تتناسب أسماؤهم في الحساب مع اسم الشركة/التجارة النظيرة، وهذا يدلّ على إتاحة غطاءٍ لحركة مبالغ كبيرة من الأموال على المستوى الدولي (ومثال ذلك قيام الشركة التي أُبلِغ عنها على أنها شركة أثاث بإجراء تحويلات كبيرة متعدّدة إلى شركة تسمى شركة تجارة النفط)
- معاملات أُجريت مع عدم تطابق المنطقة الزمنية للجهاز الذي طُلِب إجراؤها منه

الشك في الملف الشخصي لصاحب الحساب

- صاحب حساب غير راغبٍ أو غير قادر على اجتياز تحقّقات العناية الواجبة تجاه العملاء
- صاحب حساب ليس على دراية بمصدر الأموال التي تنتقل عبر حسابه أو يدّعي أنه يتعامل لصالح شخص آخر
- تغييرات متكررة في أسماء الكيانات القانونية أو الملكية الفردية باستخدام تعبيرات ومصطلحات أجنبية
- إظهار العميل أنه ليس لديه معرفة كافية بطبيعة المعاملة/المعاملات أو موضوعها أو مبلغها أو غرضها أو العلاقة بين الحسابين، أو تقديمه تفسيرات غير واقعية أو مربكة أو غير متّسقة، مما يؤدي إلى الشك في أن العميل يتصرف تصرُّف بغل المال.

الشك في هوية مستخدم الحساب

- محاولة المستخدم إخفاء هويته باستخدام هوية مشتركة أو مزورة أو مسروقة أو معدلة (العنوان، ورقم الهاتف، والبريد الإلكتروني)
- تغييرات متكررة في تفاصيل الاتصال وأرقام الهواتف وعناوين البريد الإلكتروني بعد فتح الحساب
- عناوين بريد إلكتروني لا تبدو متوافقة مع اسم صاحب الحساب، أو نمط من عناوين البريد الإلكتروني المتشابهة تَظهَر عبر حسابات متعدّدة
- وجود مخالفات في تفاصيل الملف الشخصي للعميل، مثل بيانات تسجيل الدخول المشتركة (ومثال ذلك أن تكون مشتركة بين مستخدمين أو أكثر) مع حسابات أخرى
- أمور غير طبيعية حُدِّدت من خلال السلوك عبر الإنترنت، كالتردُّد في إدخال البيانات، وتأخير ضغطات المفاتيح، وعلامات الأتمتة، وتعدّد محاولات تسجيل الدخول الفاشلة...إلخ
- حسابات متعلقة بكياناتٍ يُتوقَّع أنها لم تعد نشطة في نطاق الولاية القضائية (ومثال ذلك حساب الطلاب الأجانب بيعَ عند الفراغ من الدراسة)
- عناوين بروتوكول الإنترنت أو إحداثيات نظام تحديد المواقع العالمي (GPS) صادرة من مناطق غسل الأموال ذات المخاطر العالية
- استخدام الشبكات الخاصة الافتراضية، والأجهزة المخترقة (مثل أجهزة إنترنت الأشياء)، والشركات المُضِيفة التي قد تخفي عنوان بروتوكول الإنترنت الخاص بالمستخدم
- عناوين بروتوكول الإنترنت متعدّدة أو أجهزة إلكترونية مرتبطة بحساب واحد عبر الإنترنت
- عنوان بروتوكول الإنترنت ثابت واحد أو جهاز إلكتروني مرتبط بحسابات متعدّدة لأصحاب حسابات مختلفة
- اتصال سطح المكتب عن بُعد بالحساب من خلال منافذ الحاسوب التي تستخدمها تطبيقات مثل تيم فيوور TeamViewer وما يشبه ذلك، مما يمنع رؤية الجهاز والموقع الحقيقيين
- حسابات تُشغّل بضغطات مفاتيح أو تنقّلات سريعة للغاية سريع، وهو ما يشير إلى إمكانية أن يكون المتحكّم هو روبوت

معلومات سيئة عن صاحب الحساب

- وجود أنباء جوهرية ذات أهمية وأخبار سيئة يمكن أن يُتحقَّق منها عن العميل أو الأطراف النظيرة، ومثال ذلك وجود خبر عن حسابٍ يملكه ضحية سابقة معروفة أو مشتبه بها في نشاط احتيال أو العمل كبغل مال أو الاستيلاء على هوية

- بلاغ عن احتيال أو استرجاع احتيالي من مؤسسة مراسِلة، أو من قواعد بيانات احتيال أخرى تابعة لجهات خارجية
- ورود طلبات استرجاع حوالات برقية
- ورود معلومات سيئة مقدّمة من وحدات الاستخبارات المالية أو وكالات إنفاذ القانون حول المشاركين في المعاملة

معاملات الأصول الافتراضية

- إرسال أو استقبال كميّات كبيرة أو كميات منخفضة ولكن بتكرار كثير من الأصول الافتراضية إلى عناوين محفظةٍ غير المستضافة، أو إلى عناوين مرتبطة بأسواق الإنترنت المظلم، أو إلى منصات مواد الاعتداء الجنسي على الأطفال، أو إلى أسواق استغلال الإنترنت، أو إلى مجموعات برمجيات انتزاع الفدية، أو إلى خدمات الخلط والتقليب، أو إلى الولايات القضائية عالية المخاطر، أو إلى مواقع المقامرة، أو إلى المحتالين
- تجاوز الحد الأقصى لحدود التمويل اليومية في أجهزة الصراف الآلي الخاصة بالبيتكوين
- عدم وجود وثائق تثبت منشأ الأصول الافتراضية أو الأموال المحولة إلى أصول رقمية
- نقل أصول افتراضية إلى مَحَافظ مرتبطة بأنشطة غير قانونية على الإنترنت المظلم (كالإرهاب والمواد الإباحية المتعلقة بالأطفال والمخدرات وما إلى ذلك)
- معاملات تتضمّن أكثر من نوع واحد من الأصول الافتراضية، ولا سيّما تلك التي تتيح قدرًا أكبر من عدم الكشف عن هويته
- نشاط معاملات غير طبيعيّ للأصول الافتراضية من محافظ مرتبطة بمنصة تعمل بنظام نظير إلى نظير بدون أي تفسير تجاري منطقي

أمور أخرى

- عدم تطابق رقم الحساب واسم صاحب الحساب
- رؤية المستخدم على الهاتف أو برفقة أحد الأفراد من خلال دائرة تلفزيونية مغلقة (CCTV) يتم توجيهه أو تدريبه في أثناء إجراء المعاملة
- شركات مستفيدة تُدِير مواقع إنترنت مزوّدة لخدمات التداول والاستثمار، تكون في كثير من الحالات غير مرخّصة أو مُدرجَة في قائمة هيئة الرقابة المحلية

الملحق ب: بيان ارتباط أوجه التآزر بين ضوابط مكافحة الاحتيال ومكافحة غسل الأموال وتمويل الإرهاب

يجمع هذا الملحق بعض الأمثلة الجيدة لكيفية اعتماد الهيئات التنظيمية المالية لمتطلبات مكافحة الاحتيال إلى جانب ضوابط مكافحة غسل الأموال وتمويل الإرهاب، ويستهدف بعضها قدرةَ المجرمين على تسجيل الحسابات الوهمية والوصول إليها والتحكم فيها عن بُعد. ويشتمل ذلك على تدابير شتّى متعلقة بالتحقّق من العملاء ورصد المعاملات.

وقد تُفِيد هذه الضوابط المؤسسات المالية ومزوّدي خدمات الأصول الافتراضية ومؤسسات الدفع الأخرى.

- تثبيت عمليات حازمة لتقنية اعرف عميلك (KYC) أو اعرف عملك التجاري، وميزات الاستدلال الحيوي (biometric) أثناء عملية الانضمام الرقمي وما إلى ذلك، والتحقق من جهاز محمول واحد أو جهاز آمن واحد لمصادقة المعاملات المصرفية عبر الإنترنت (وتُحظَر الأجهزة الأخرى أو تُخضَع لتدابير معزِّزة لتخفيف المخاطر).
- فرض فترة السماح بإلغاء الحساب (cooling-off period) للتسجيل أوّل مرة في الخدمات المصرفية عبر الإنترنت أو الأجهزة الآمنة (ومعنى هذه الفترة ألّا تُتَاح المجموعة الكاملة من الخدمات المصرفية على الفور عند فتح الحساب)، وهذا يحدّ من عدد المعاملات المالية للعميل أو قيمة مبالغها.
- وضع تعريف للمعاملات المتوقعة (عدد المعاملات، ومبالغها، وأنواع الأطراف النظيرة، والبلدان الداخلة في المعاملة) فذلك يُعِين على اكتشاف المعاملات المشبوهة، إضافةً إلى تشديد قواعد الكشف عن الاحتيال ومحفزاته لحظر المعاملات غير المشروعة حظرًا اسباقيًّا.
- استخدام خدمات "التحقق من المستفيد"، فهي تتيح لمُصدِر أمر التحويل أو الدافع أو المدين التحقّق من تطابق المستفيد أو المدفوع إليه أو الدائن المذكور في رسائل الدفع مع اسم صاحب الحساب.
- تقليل أي اتّصال عبر البريد الإلكتروني ووسائل التواصل الاجتماعي مع العملاء والاقتصار على المعلومات العامة فقط، مع النصّ صراحةً على عدم تبادل أي بيانات تعريفية أو شخصية عبر البريد الإلكتروني مع المؤسسة المالية أو مزوّد خدمات الأصول الافتراضية.
- إضافة برنامج التعرّف على الصوت ودعم الذكاء الاصطناعي في التواصل مع العملاء للتأكد من هويتهم الحقيقية.
- اشتراط آليات استيقان متعدّدة العوامل للتحقّق من العملاء ولإجراء المعاملات المالية ولإضافة المستفيدين أو لتفعيلهم، باستخدام قنوات مختلفة.
- التحقّق من هوية المستخدم أثناء الإعداد الحساب عن بُعد ومنع المجرمين من الوصول إلى حسابات متعدّدة باستخدام معلومات حسابات بغال المال أو الضحايا، وذلك من خلال:
  - تعزيز الموثوقية في عملية تحديد هوية العميل من خلال الاختبارات الحيوية (وهي اختبارات تضمن أن الذي تجري عليه إنسان حيّ وحقيقيّ)، ومن ذلك اختبار ما إذا كان الفرد قد خضع لتقنية الهندسة الاجتماعية خلال التحققات الحيوية.
  - رصد عناوين بروتوكول الإنترنت المستخدمة للاتصال بمواقع الخدمات المصرفية عبر الإنترنت، وما إلى ذلك، ومن ذلك الكشفُ عن استخدام أدوات الوصول عن بُعد وعن الهجوم الذي يسمّى "رجلٌ في المتصفح".
- توسيع أنواع البيانات التي تجمعها الكيانات المبلّغة عن العملاء وتحلِّلها، ومنها على سبيل المثال أرقام الهواتف المحمولة وعناوين بروتوكول الإنترنت وإحداثيات نظام تحديد المواقع العالمي (GPS) ومعرّف الجهاز، وما إلى ذلك. ولأغراض الوقاية من الاحتيال، يمكن للمؤسسات المالية تكرار هذا التحديد باستخدام نهج قائم على المخاطر (ومثال ذلك أن تُجرِيَ عمليات التحقّق هذه عند كشف سلوك غير طبيعي).
- تطبيق نظام رصدٍ للمعاملات آنيّ قائمٍ على المخاطر، وذلك لضمان سرعة الكشف عن أي نشاط غير طبيعي والتحقيق فيه والإبلاغ عنه عند الاقتضاء من خلال تقديم تقرير عن المعاملات المشبوهة. ولا بدّ من أن يتناسب تطوُّر نظام الرصد هذا مع مقدار وطبيعة المعاملات التي تتناولها المؤسسة المالية.

EGMONT GROUP
OF FINANCIAL INTELLIGENCE UNITS

INTERPOL

FATF

www.egmontgroup.org | www.interpol.int | www.fatf-gafi.org

تشرين الثاني/نوفمبر 2023

التدفقات المالية غير المشروعة الناجمة عن الاحتيال الذي يسهل الإنترنت ارتكابها