الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

Q.5051

(2020/03)

السلسلة Q: التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما

مكافحة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة والمسروقة

إطار من أجل مكافحة استخدام الأجهزة المتنقلة المسروقة

التوصية ITU-T Q.5051

توصيات السلسلة Q الصادرة عن قطاع تقييس الاتصالات

التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما

التشوير في الخدمة اليدوية الدولية	Q.3–Q.1
التشغيل الدولي الأوتوماتي وشبه الأوتوماتي	Q.59–Q.4
الوظائف وتدفق المعلومات في خدمات الشبكات الرقمية المتكاملة الخدمات (ISDN)	Q.99–Q.60
البنود المطبقة على الأنظمة المعمارية في قطاع تقييس الاتصالات	Q.119–Q.100
مواصفات أنظمة التشوير رقم 4 و5 و6 وR1 وR2	Q.499–Q.120
البدالات الرقمية	Q.599–Q.500
التشغيل البيني في أنظمة التشوير	Q.699–Q.600
مواصفات نظام التشوير رقم 7	Q.799–Q.700
السطح البيني Q3	Q.849–Q.800
نظام التشوير الرقمي رقم 1 للمشترك	Q.999–Q.850
الشبكات المتنقلة البرية العمومية	Q.1099–Q.1000
التشغيل البيني مع الأنظمة المتنقلة الساتلية	Q.1199–Q.1100
الشبكة الذكية	Q.1699–Q.1200
متطلبات وبروتوكولات التشوير للأنظمة المتنقلة الدولية–2000	Q.1799–Q.1700
مواصفات التشوير المتعلقة بتحكم في النداء مستقل عن حامل النداء (BICC)	Q.1999–Q.1900
الشبكة ISDN عريضة النطاق	Q.2999–Q.2000
متطلبات وبروتوكولات التشوير لشبكات الجيل التالي	Q.3709–Q.3000
متطلبات وبروتوكولات التشوير للشبكات المعرفة بالبرمجيات	Q.3899–Q.3710
مواصفات الاختبار	Q.4099–Q.3900
متطلبات وبروتوكولات التشوير للأنظمة المتنقلة الدولية–2020	Q.5049–Q.5000
مكافحة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة والمسروقة	**Q.5069–Q.5050**

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T Q.5051

إطار من أجل مكافحة استخدام الأجهزة المتنقلة المسروقة

ملخص

تقترح هذه التوصية ITU-T Q.5051 إطاراً يتكون من المتطلبات ومجموعة واسعة من التدابير الشاملة والموصى بها التي يمكن اتخاذها وتطبيقها لمكافحة سرقة الأجهزة المتنقلة وإعادة استخدام الأجهزة المسروقة.

وتماشياً مع تنامي الوظائف والقدرات المتاحة على الأجهزة المتنقلة، تزايدت في السنوات الأخيرة أهمية هذه الأجهزة واستخدامها في حياة الناس اليومية. ومن حيث الآثار الجانبية المترتبة على ذلك، لوحظ أيضاً تزايد أعمال السرقة التي تستهدف هذه الأجهزة، في بعض البلدان، وجني الأرباح منها ليس عن طريق بيع المعدات نفسها فحسب، بل أيضاً باستخدام المعلومات التي تحتويها المعدات استخداماً غير قانوني.

وسعياً للتصدي لهذه الظاهرة، ثمة حاجة إلى مبادرات لردع سرقة وإعادة استعمال الأجهزة المسروقة المتنقلة وحماية بيانات المستهلك المخزنة على هذه الأجهزة من الاستخدام غير القانوني لها. ومن الشائع كذلك أن تُسرق أجهزة في بلد معين، يكون قد طور حلولاً للحد من استعمال هذه الأجهزة المسروقة، بحيث تباع في بلدان أخرى أو حتى في مناطق قد لا تكون قد اتخذت فيها تدابير تخفيف مماثلة. لذلك، من الأهمية بمكان لنجاح مثل هذه المبادرات أن يكون هناك تنسيق وتبادل للمعلومات بين الحكومات والمشغلين يهدف إلى مكافحة سرقة الأجهزة المتنقلة وإعادة استعمال الأجهزة المسروقة في بيئة عالمية. وبدون ذلك، ستكون هناك مخاطر حدوث الاتجار غير المشروع بالأجهزة المسروقة عبر الحدود الدولية.

ويجدر بالذكر أن معظم الحلول التي تُقدَّم اليوم لمنع سرقة الأجهزة وإعادة استخدامها تعتمد على قوائم معرّفات الهوية الفريدة. والإجراء الشائع الذي يلجأ إليه التجار غير الشرعيين عندئذ لتجاوز هذه الإجراءات هو التلاعب بالجهاز لتغيير معرّف هوية فريد، وأحياناً اختيار معرّف هوية مستخدم بالفعل في جهاز شرعي. ويتيح ذلك إعادة الجهاز إلى السوق وتوصيله بالشبكات المتنقلة.

واستجابة لهذا السيناريو، فإن العديد من البلدان لا تشترك في مكافحة استخدام الأجهزة المتنقلة المسروقة فحسب، بل أيضاً في منع الأجهزة ذات معرّفات الهوية الفريدة المعاد برمجتها بدون ترخيص والتي توصف عموماً كمعرّفات مغشوشة، من العودة إلى الشبكة. وفي الوقت نفسه، تواجه بعض الحكومات في بلدان أخرى تحديات صعبة وعدم وضوح بشأن أفضل الاستراتيجيات التي يتعين اعتمادها، ويرجع ذلك أساساً إلى الافتقار إلى المعرفة أو الخبرة لفهم المشكلة أو الحلول المتاحة، وإلى اتخاذ الخيارات المستنيرة لنشر حلول مصممة خصيصاً لبلدانهم، والتي يمكن أن تكون فعالة. وبهذا المعنى، تصبح المبادئ التوجيهية ضرورية للتصدي لهذا التحدي، على النحو المشار إليه في القرار 97 (الحمامات، 2016) للجمعية العالمية لتقييس الاتصالات.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T Q.5051	2020-03-13	11	11.1002/1000/14140

مصطلحات أساسية

مكافحة الأجهزة المتنقلة المسروقة، مطابقة، إطار، متطلبات، أمن.

---

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T Q.5051

إطار من أجل مكافحة استخدام الأجهزة المتنقلة المسروقة

1 مجال التطبيق

تشمل هذه التوصية الإطار المرجعي والمتطلبات التي ينبغي النظر فيها لدى نشر الحلول لمكافحة استخدام الأجهزة المتنقلة المسروقة.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع للمراجعة، يرجى من جميع المستخدمين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية حالياً. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T Q.5050] التوصية ITU-T Q.5050 (2019)، *إطار حلول لمكافحة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة*.

[ITU-T X.1058] التوصية ITU-T X.1058 (2017)، *تكنولوجيا المعلومات – التقنيات الأمنية – مدونة القواعد لحماية المعلومات المحدِّدة لهويّة الشخص*.

[ITU-T X.1127] التوصية ITU-T X.1127 (2017)، *المتطلبات الأمنية الوظيفية والمعمارية الوظيفية لتدابير مكافحة سرقة الهواتف المتنقلة*.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 مستعمل الجهاز (device user) [ITU-T X.1127]: المستعمل المخوَّل للجهاز.

2.1.3 مفتاح التعطيل (kill switch) [b-GSMA]: "مفتاح التعطيل" هو طريقة لتعطيل وظائف هامة للغاية داخل جهاز متنقل. وهو باختصار وظيفة داخل الجهاز المتنقل، بحيث إذا فُعِّلت مثلاً برسالة ذات نسق ما تُرسَل إليه، يتوقف الجهاز المتنقل عن العمل على النحو المقصود منه، ولا تتسنى إعادة تفعيله أو إعادة استعمال إلا إذا صرح مالك الجهاز بإعادة تفعيله.

3.1.3 الهاتف المتنقل (mobile phone) [b-ITU-T X.Sup.19]: جهاز إلكتروني يُستخدم لإجراء النداءات الهاتفية وإرسال الرسائل النصية عبر منطقة جغرافية واسعة عن طريق النفاذ الراديوي إلى الشبكات المتنقلة العمومية، مع تمكين المستعمل من التنقل.

4.1.3 الهاتف الذكي (smartphone) [b-ITU-T X.Sup.19]: هاتف متنقل بقدرات حوسبة قوية وتوصيلية بين أطراف غير متجانسة ونظام تشغيل متقدم يوفر منصة لتطبيقات الأطراف الثالثة.

5.1.3 جهاز تكنولوجيا المعلومات والاتصالات المغشوش (tampered ICT device) [ITU-T Q.5050]: هو جهاز لتكنولوجيا المعلومات والاتصالات (ICT) يتضمن مكونات أو برمجيات أو معرفات هوية فريدة أو أجزاء تحميها حقوق الملكية الفكرية أو علامات تجارية تعرضت للتغيير مبدئياً أو فعلياً دون موافقة صريحة من الجهة المصنعة أو ممثلها القانوني.

6.1.3 معرّف الهوية الفريد (unique identifier) [ITU-T Q.5050]: معرّف هوية يرتبط بجهاز واحد ويهدف إلى تعريف هوية بصورة متفردة.

2.3 مصطلحات معرفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 معرّف الهوية غير الصالح (invalid identifier): هو معرّف هوية فريد لا يمتثل للنسق المحدد في المعايير التقنية أو غير مدرج في قاعدة البيانات المرجعية لمعرّفات هوية الأجهزة التي توزعها الجهة الإدارية المسؤولة.

2.2.3 معرّف الهوية المستنسخ (cloned identifier): هو معرّف هوية جهاز صالح تخصّصه لجهاز واحد بشكل صحيح الجهة الإدارية المسؤولة ولكنه مستعمل من جانب أجهزة مختلفة أخرى.

3.2.3 معرّفات الهوية الفريدة الموثوقة (reliable unique identifiers): يجب أن تكون فريدة لكل من المعدات التي تهدف إلى تعريف هويتها، وألا تخصصها إلا جهة إدارية مسؤولة، وينبغي ألا تغيره أطراف غير مرخص لها بذلك.

4 المختصرات والمختزلات

تستخدم هذه التوصية المختصرات والمختزلات التالية:

EIR سجل هوية المعدات *(Equipment Identity Register)*

IMEI الهوية الدولية للمعدات المتنقلة *(International Mobile Equipment Identity)*

IMSI الهوية الدولية للمشترك المتنقل *(International Mobile Subscriber Identity)*

PII المعلومات المحدِّدة لهوية الشخص *(Personally Identifiable Information)*

RUI معرّف الهوية الفريد الموثوق *(Reliable Unique Identifier)*

TAC شفرة توزيع النمط *(Type Allocation Code)*

5 الاصطلاحات

تطبق هذه التوصية الأشكال الشفهية التالية لتعابير النصوص:

أ) في هذه التوصية كلمة "مطلوب" تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم المطابقة مع هذه الوثيقة.

ب) وتدل "ينبغي" و"يوصى" على متطلب يوصى به لكنه غير إلزامي بالمطلق. وبالتالي لا حاجة تدعو لتوفر هذا المتطلب لزعم المطابقة.

ج) وكلمة "يجوز" تدل على مطلب اختياري مسموح به دون أن ينطوي على أي توصية به. ولا يرمي هذا المصطلح إلى إلزام تنفيذ البائع بتوفير هذا الخيار الذي يمكن أن يفعّله مشغل الشبكة/مقدم الخدمة بشكل اختياري. بل إن المصنّع يمكنه إدراج هذا الخيار وزعم المطابقة مع هذه التوصية في نفس الوقت.

6 الجوانب العامة

تماشياً مع تنامي الخواص الوظيفية والقدرات المتاحة على الأجهزة المتنقلة، تزايدت في السنوات الماضية أهمية هذه الأجهزة واستخدامها في حياة الناس اليومية. ومن حيث الآثار الجانبية المترتبة على ذلك، لوحظ أيضاً تزايد أعمال السرقة التي تستهدف هذه الأجهزة، في بعض البلدان، وجني الأرباح منها ليس عن طريق بيع المعدات نفسها فحسب، بل أيضاً باستخدام المعلومات التي تحتويها المعدات استخداماً غير قانوني.

وسعياً للتصدي لهذه الظاهرة، ثمة حاجة إلى مبادرات لردع سرقة وإعادة استعمال الأجهزة المتنقلة وحماية بيانات المستهلك المخزنة على هذه الأجهزة من استخدامها بشكل غير قانوني. ولما كان من الشائع كذلك أن تُسرق أجهزة في بلد معين، يكون قد طور حلولاً للحد من استعمال هذه الأجهزة المسروقة، بحيث تباع في بلدان أخرى أو حتى في مناطق قد لا تكون قد اتخذت فيها تدابير تخفيف مماثلة. لذلك، فمن الأهمية بمكان لنجاح مثل هذه المبادرات أن يكون هناك تنسيق وتبادل للمعلومات بين الحكومات والمشغلين من مختلف البلدان التي تهدف إلى مكافحة سرقة الأجهزة المتنقلة وإعادة استعمال الأجهزة المسروقة في بيئة عالمية. وبدون ذلك، ستكون هناك مخاطر ناجمة عن تسهيل الاتجار غير المشروع بالأجهزة المسروقة عبر الحدود عن غير قصد.

واستجابة لهذا السيناريو، فإن العديد من البلدان لا تشترك في مكافحة استخدام الأجهزة المتنقلة المسروقة فحسب، بل أيضاً في منع الأجهزة ذات معرّفات الهوية الفريدة المعاد برمجتها بدون ترخيص والتي توصف عموماً كمُعرّفات مغشوشة، من العودة إلى شبكة الاتصالات المتنقلة. وفي الوقت نفسه، تواجه بعض الحكومات في بلدان أخرى تحديات صعبة وعدم وضوح بشأن أفضل الاستراتيجيات التي يتعين اعتمادها، ويرجع ذلك أساساً إلى الافتقار إلى المعرفة أو الخبرة لفهم المشكلة أو الحلول المتاحة، وإلى اتخاذ الخيارات المستنيرة لنشر حل مصمم خصيصاً لبلدانهم، والتي يمكن أن تكون فعالة. وبهذا المعنى، تصبح التوصيات ضرورية للتصدي لهذا التحدي، على النحو المشار إليه في القرار 97 (الحمامات، 2016) للجمعية العالمية لتقييس الاتصالات (WTSA).

لذلك، تصف هذه التوصية إطاراً يتكون من المتطلبات ومجموعة واسعة من التدابير الشاملة والموصى بها التي يمكن اتخاذها وتطبيقها لمكافحة سرقة الأجهزة المتنقلة وإعادة استخدام الأجهزة المسروقة.

7 المتطلبات الإجمالية

تتعدد التحديات التي يواجهها أصحاب المصلحة عند نشر حلول للتصدي لاستخدام الأجهزة المتنقلة المسروقة. وعند نشر حلول لمكافحة استخدام الأجهزة المتنقلة المسروقة، تنبغي للبلدان مراعاة المتطلبات الواردة في هذه الفقرة.

1.7 منع المستعملين غير المخوَّلين من استعمال الأجهزة المتنقلة المسروقة

يلزم تنفيذ حلول تهدف إلى إلغاء تفعيل الأجهزة في حالة سرقتها أو فقدها، وجعلها غير قابلة للتشغيل من قبل مستعملين غير مخوَّلين.

- يلزم أن تجرى هذه العملية أوتوماتياً بعد أن يحاول مستعمل غير مخوَّل النفاذ إلى الجهاز لعدد محدد من المرات (على سبيل المثال إذا فشل المستعمل غير المخوَّل في إدخال كلمة السر أو رقم تعرّف الهوية الشخصي (PIN) بعد عدد معين من المحاولات).
- يوصى بأن يتسنى للمستعمل المخوَّل تفعيل هذه العملية عن بُعد عند الحاجة (على سبيل المثال عن طريق تشغيل وظيفة مفتاح التعطيل على الجهاز المفقود/المسروق).
- يلزم وجود خيار لوقف قابلية عدم التشغيل إذا استرد مستعمل الجهاز المخوَّل جهازه ولاستعادة بيانات المستعمل على الجهاز إلى أقصى حد ممكن.

وتتناول التوصية [ITU-T X.1127] متطلبات الأمن الوظيفي ومعماريته فيما يتعلق بتدابير مكافحة السرقة القائمة على الهواتف المتنقلة. وتصف تلك التوصية تنفيذ أداة مفتاح التعطيل لاستخدامها في حالة ضياع أي هاتف ذكي أو سرقته. وينبغي أن تقدم هذه الأداة القدرات التالية:

- الحذف عن بُعد لبيانات المستخدم المخوَّل الموجودة على الهاتف الذكي؛
- جعل الهاتف الذكي غير صالح للعمل من جانب مستخدم غير مخوَّل؛
- منع إعادة التفعيل دون إذن المستخدم المخوَّل إلى أقصى حد ممكن من الناحية التكنولوجية؛
- معاودة جعل الهاتف الذكي صالحاً للعمل إذا استعاده المستخدم المخوَّل، واستعادة بيانات المستخدم على الهاتف الذكي إلى أقصى حد ممكن؛
- إتاحة تتبع موقع الجهاز المتنقل المفقود أو المسروق.

ويوصى بتعليم مستعملي الأجهزة المتنقلة كيفية تشكيل واستخدام هذه الخواص الوظيفية وكيفية الإبلاغ عن أجهزتهم المتنقلة المفقودة/المسروقة لموردي الخدمات أو الشرطة المختصة أو السلطات القضائية، وذلك لمنع هذه الأجهزة من النفاذ إلى الشبكات المتنقلة وتمكين وكالات إنفاذ القانون من اتخاذ الإجراءات المناسبة.

2.7 منع الأجهزة المتنقلة المسروقة من النفاذ إلى الشبكة

يلزم تنفيذ حلول لمنع الأجهزة المتنقلة المسروقة من النفاذ إلى الشبكات المتنقلة، ويُفضل أن يجري ذلك من خلال أنظمة مؤتمتة قابلة للمراجعة.

ويلزم أن يكون بإمكان الأشخاص المخوَّلين فقط، مثل المالك الشرعي للجهاز، طلب إدراج جهاز متنقل مسروق في جميع الشبكات في البلد أو إزالته منها.

ويوصى بوضع إطار سياساتي لمنع استخدام الأجهزة المسروقة على الشبكات.

ومن المهم الإشارة إلى أن الأجهزة التي يتم حجبها على الشبكات المتنقلة، باستخدام معرّفات هويتها الفريدة، لا يزال بإمكانها النفاذ إلى الشبكات التي لا تتحقق من معرّفات الهوية الفريدة للجهاز المتنقل، مثل شبكات Wi-Fi. ولذلك، من المهم استكمال هذا النهج بالنُهج الأخرى مثل تلك الوارد وصفها في الفقرة 1.7.

3.7 منع استخدام الأجهزة المتنقلة ذات معرّفات الهوية الفريدة المغشوشة و/أو المستنسخة

يلزم تنفيذ حل لتحديد الأجهزة المتنقلة ذات معرّفات الهوية الفريدة المغشوشة و/أو المستنسخة وتمييزها عن الأجهزة الأصلية، بدقة عالية، بغية التمكن من اتخاذ إجراءات معطلة، ويُحبذ أن تكون من خلال أنظمة مؤتمتة، دون أن يكون لها تأثير على الأجهزة الأصلية.

ويوصى بأن تمثل قواعد البيانات المرجعية جزءاً من هذا الحل من أجل تحديد المعلومات الخاصة بالأجهزة الأصلية ومنشأها القانوني. وينبغي استخدام قواعد بيانات التسجيل الوطنية لتحديد الأجهزة المستوردة والمقتناة بشكل قانوني، وقواعد بيانات معرّفات الهوية المخصصة للمصنعين والخصائص الأخرى للأجهزة بوصفها مصدر المعلومات لقاعدة البيانات المرجعية لتسهيل تمييز الأجهزة الأصلية عن الأجهزة المغشوشة.

ويلزم في هذا الحل مراعاة أن معرّف الهوية المغشوش يمكن أن يكتسب أشكالاً مختلفة يتعين مواجهتها في عملية الكشف والسيطرة، مثل معرّفات هوية غير صالحة، ومستنسخة، وعند الاقتضاء، وذات نوع غير معتمد، وغير مسجلة في قواعد البيانات المرجعية الوطنية.

4.7 منع الأجهزة المتنقلة المسروقة من بلدان أخرى من النفاذ إلى الشبكة

يوصى بأن تسهل القوانين واللوائح المحلية التنسيق وتبادل المعلومات بين الحكومات والمشغلين من مختلف البلدان لمنع استخدام الأجهزة المسروقة، بصرف النظر عن المكان الذي سرقت منه.

ويتيح الإخفاق في تشجيع تبادل البيانات وتسهيلها على الصعيد الدولي إلى الاستمرار في عدم ضبط الاتجار غير القانوني بالأجهزة المسروقة على الصعيد الدولي مؤدياً إلى تصدير الأجهزة المسروقة في بلد معين إلى بلدان أو مناطق أخرى وبيعها فيها.

ويوصى بوجود قاعدة بيانات عالمية للأجهزة المسروقة يمكن النفاذ إليها من قبل جميع الجهات من أي مكان في العالم للإبلاغ عن الأجهزة المسروقة والتحقق من سرقة أي جهاز، وذلك للتصدي لهذه القضية وحلها.

وينبغي تبادل القوائم السوداء للأجهزة المحلية الوطنية وإتاحتها للمجتمع العالمي من خلال الإلزام بالإبلاغ عن الأجهزة المحلية المسروقة وإدخال بياناتها في قاعدة البيانات العالمية للأجهزة المسروقة.

5.7 الحد من الآثار على المستهلك

تنبغي مراعاة الآثار على المستهلك عند اعتماد أي حل يرمي إلى مكافحة استخدام الأجهزة المتنقلة المسروقة. وعندما تتاح نُهج متعددة للمستهلك لتحقيق الهدف نفسه، ينبغي أن يُعتمد الحل الذي يحد من الآثار الإجمالية على المستهلكين الشرعيين.

ويوصى بالسيطرة على الأجهزة ذات معرفات الهوية غير الصالحة والمفعلة حديثاً على الشبكات وبتقديم تبليغ مسبق للمستعملين، مع منحهم متسعاً كافياً ومناسباً من الوقت لتقديم دليل على الملكية القانونية والحد من آثار رفض الخدمة الفجائي لهذه الأجهزة أو تفادي هذه الآثار تماماً.

ويوصى بتفادي حجب اشتراك الخدمة للمستعمل عند اتخاذ تدابير للسيطرة على الأجهزة ذات معرّفات الهوية المغشوشة و/أو المستنسخة.

ويوصى بنشر الحملات التثقيفية وحملات التوعية على نحو علني بكل الوسائل المتاحة بشأن التدابير التي يتعين اتخاذها، والهدف منها، وفوائدها، والخيارات والإجراءات التي يمكن أن يلجأ إليها المستعملون في حالة فقدان أجهزتهم اليدوية الخاصة أو سرقتها، أو في حالة امتلاك أجهزة ذات معرّفات هوية مغشوشة أو مستنسخة.

ويوصى عند اعتماد تدابير لمكافحة الأجهزة ذات معرّفات الهوية المغشوشة و/أو المستنسخة بأن تراعي فترة سماح أو فترة انتقال. حيث إن الأجهزة المستعملة بالفعل يمكن أن تكون قد اقتنيت عن حسن نية ومستعملوها لا يدركون المخاطر التي يمكن أن تمثلها. وإذا تقرر عدم إيقاف تشغيل الأجهزة القديمة، ينبغي اتخاذ تدابير إضافية لتفادي تفعيل هذه الأجهزة من قبل مستعملين جدد.

ويوصى باتباع أساليب فعالة للحصول على تقارير ومعلومات تخص المستعملين واتخاذ الإجراءات الكفيلة بتعليق الخدمات وحجب معرّفات هوية الأجهزة.

ويوصى بتسهيل حجب معرّف هوية الجهاز دون مطالبة المستعمل بتذكره أو البحث عنه. وذلك، على سبيل المثال، بالبحث في وظيفة تسجيل المكالمات في الجهاز في شبكة المشغل لتحديد معرّف الهوية المفقود/المسروق.

ويوصى بتعليق الخدمات وحجب معرّفات هوية الجهاز المفقود/المسروق في أسرع وقت ممكن. فعلى سبيل المثال، يتم إيقاف الجهاز عن العمل بمجرد أن يقوم أصحاب المصلحة المسؤولون عن إيقاف الجهاز عن العمل بتأكيد صحة الطلب.

ويُطلب توفير الأدوات اللازمة لجميع أصحاب المصلحة للتحقق من إيقاف الجهاز عن العمل والتأكد من ذلك.

ويوصى صاحب المصلحة المسؤول عن إيقاف الجهاز عن العمل بالرد على المستعمل عندما يتم وقف الجهاز من الخدمة أو ذكر أسباب عدم إيقاف الجهاز المبلغ عنه عن العمل إذا ما تم رفض الطلب.

6.7 حماية بيانات المستهلك الخاصة

ينبغي حماية بيانات المستهلك الخاصة في حالة فقدان الجهاز أو سرقته. وكإجراء أولي، يُوصى بتنفيذ آليات لحظر تشغيل الجهاز بما في ذلك نفاذ مستعمل غير مخوَّل إلى البيانات الخاصة التي الموجودة على الجهاز.

ويوصى بتثقيف المستهلكين بشأن أهمية حماية بياناتهم الشخصية وإنشاء نسخ احتياطية لها، وبشأن استخدام الوظائف التي تسمح لهم بمسح المعلومات الشخصية (PII) عن بُعد من على الجهاز المسروق.

ويوصى أن يدرج المصنعون سمات التوصية [ITU-T X.1127] على جميع الأجهزة الجديدة على نحو تلقائي.

كما يوصى بأنه يقوم أصحاب المصلحة بتثقيف المستهلكين بشأن كيفية تشكيل هذه الوظيفة واستخدامها.

7.7 منع وصول الأجهزة المتنقلة المسروقة إلى الأسواق

يوصى بأن تتعاون الوكالات الوطنية لتنظيم الاتصالات مع الوكالات الوطنية المعنية الأخرى (مثل الجمارك) لتحسين عمليات مراقبة الأجهزة المبلغ عن فقدانها أو سرقتها على المستوى الوطني وفي البلدان الأخرى.

وفي إطار هذا التعاون، ينبغي النظر في تقديم ما يلي، حسب الاقتضاء:

1) النفاذ إلى قواعد بيانات الأجهزة المسروقة، إضافة إلى المعلومات الإضافية (مثلاً، الأجهزة غير الصالحة، أو من نوع غير معتمد) نظراً لأنه يمكن تغيير معرّف الهوية الفريد لتجاوز قواعد البيانات الوطنية والدولية للأجهزة المسروقة؛

2) النفاذ إلى قاعدة بيانات عالمية لمعرّفات الهوية المخصصة للجهات المصنعة المشروعة، من أجل التحقق من صحة بنية معرّفات الهوية الخاصة بالأجهزة التي ستُستورد؛

3) النفاذ إلى قائمة العلامات التجارية للأجهزة المعتمدة النوع وطرزها للسماح فقط باستيراد طرازات الأجهزة المعتمدة النوع وفقاً للوائح الوطنية ذات الصلة؛

4) النفاذ إلى قواعد البيانات المرجعية الوطنية التي تحتوي على سجل لمعرّفات هوية الأجهزة المستوردة المملوكة شرعياً، حسب الاقتضاء؛

5) النفاذ إلى قاعدة بيانات عالمية للأجهزة المسروقة إلى جانب النفاذ إلى قاعدة بيانات توفر معلومات خاصة بالجهاز للقدرة على تأكيد استيقان الأجهزة. وستكون هذه العملية الأخيرة مفيدة في الحالات التي يتعرض فيها معرّف الهوية الفريد للجهاز للتغيير وإعادة البرمجة باستخدام معرّف هوية لجهاز مختلف.

ويوصى بتدقيق معرّف الهوية الكامل بمقارنته مع قاعدة البيانات الوطنية للأجهزة، لتجنب دخول جهاز ذي معرّف هوية خاص بجهاز آخر دخل البلد بالفعل.

ويوصى باتخاذ إجراءات قانونية ضد مراكز البيع التي تعرض أجهزة مسروقة للبيع.

8.7 الاعتبارات الأخرى للتصدي للتلاعب بمعرّفات الهوية الفريدة للأجهزة المتنقلة المسروقة

يمكن أن تشمل الاعتبارات الأخرى للتصدي للتلاعب بالأجهزة المتنقلة المسروقة ما يلي:

- النظر في وضع أطر سياساتية لمنع استخدام الأجهزة المتنقلة المسروقة المغشوشة أو بيعها في السوق؛
- توفير التعليم والتدريب بشأن الجوانب التقنية المتعلقة بسرقة معرّفات الهوية الفريدة للأجهزة والتلاعب بها؛
- النظر في الضوابط بشأن استخدام العتاد و/أو البرمجيات المستخدمة للتلاعب بمعرّفات هوية الأجهزة المتنقلة.

ويوصى بتوفير أسس قانونية ودعم لكي يتسنى لسلطات إنفاذ القانون معاقبة من يغيرون معرّفات هوية الأجهزة المتنقلة أو يقومون بتعديلها أو تزويرها أو محوها أو التلاعب بها، بهدف التحايل على الإجراءات المتبعة لمنع استخدام الأجهزة المسروقة في السوق.

ويوصى بأن يشمل هذا الإطار القانوني أيضاً الإجراءات التي يمكن اتخاذها ضد من يعرضون العتاد و/أو البرمجيات المستخدمة في التلاعب بمعرفات هوية الأجهزة المتنقلة، أو يمتلكونها أو يستوردونها أو يبيعونها.

ويوصى أيضاً بتعليم سلطات إنفاذ القانون وتدريبها بشأن الجوانب التقنية المتعلقة بسرقة معرّفات الهوية الفريدة للأجهزة المتنقلة والتلاعب بها، والإطار القانوني للسماح بتجريم هذه الأفعال.

ويوصى لمصنعي الأجهزة المتنقلة بتضمين آليات لضمان موثوقية وسلامة المعرفات الفريدة للأجهزة المتنقلة.

8 متطلبات الإطار

عند نشر حلول للتعامل مع الأجهزة المتنقلة المسروقة، ينبغي أن تراعى المتطلبات التالية.

8.1 قاعدة بيانات مرجعية مركزية

يوصى باستخدام قاعدة بيانات مرجعية مركزية لتخزين المعلومات الخاصة بالأجهزة المفقودة أو المسروقة. وبالتالي، ينبغي أن تستفيد جميع شركات الاتصالات من قاعدة البيانات هذه لمنع الأجهزة المسروقة من النفاذ إلى أي شبكة متنقلة. وينبغي أن تتضمن قاعدة البيانات هذه، على أقل تقدير معرّف الهوية الفريد للجهاز المسروق، وتاريخ السرقة والجهة التي أدخلت المعلومات في قاعدة البيانات.

ويوصى أن تتضمن قاعدة البيانات هذه أيضاً أنواعاً أخرى من معرّفات الهوية والمعلومات للمساعدة في تحديد الأجهزة المسروقة ذات معرّفات الهوية المغشوشة والتعامل معها.

ويوصى بإدراج معلومات تتعلق بالأجهزة المستوردة و/أو المملوكة شرعياً في قاعدة البيانات المرجعية.

ويوصى بأن يكون للجهات المخوَّلة القدرة على النفاذ إلى جميع قواعد البيانات ذات الصلة.

ويوصى بتطبيق التسجيل الإلزامي للأجهزة. وعند القيام بذلك، ينبغي إيلاء الاعتبار الواجب عند الربط بين الجهاز والمعلومات المحددة لهوية الأشخاص، وللآثار الجانبية على تجارة الأجهزة المتنقلة القانونية والمنافسة في سوق الأجهزة المتنقلة.

ويوصى بتنفيذ إجراءات التدقيق للتحقق من حجب الأجهزة المسروقة المبلغ عنها ومما إذا كان جميع أصحاب المصلحة قد اعتمدوا الإجراءات السليمة.

2.8 شبكة الدعم لحجب الأجهزة

من اللازم أن تحتوي الشبكات المتنقلة على عناصر قادرة على منع نفاذ الأجهزة المسروقة التي أدرجت معرّفات هويتها الصالحة في القائمة السوداء وأيضاً الأجهزة التي ترسل معرّفات هوية بأنساق لا تمتثل لمعايير معرّفات الهوية الفريدة.[1]

ويوصى بأن تدعم حلول الحجب المستخدمة في الشبكات المتنقلة سمات لتجنب استخدام الأجهزة ذات معرّفات الهوية الفريدة المستنسخة وبالتالي التمييز بين الأجهزة الأصلية والمستنسخة.[2]

3.8 معرّفات الهوية الفريدة الموثوقة – RUI

يوصى بأن تستند قواعد البيانات المرجعية المستخدمة لمنع نفاذ الأجهزة المحمولة المسروقة إلى الشبكات المتنقلة، إلى مُعرّفات هوية فريدة موثوقة (RUI)، لأن التلاعب بمُعرّفات الهوية الفريدة (RUI) للأجهزة يمكن أن يؤثر سلباً على كفاءة الحلول التي تهدف إلى إبعاد الأجهزة المسروقة من السوق.

ويوصى بأن تخزن[3] الأجهزة المتنقلة معرّف الهوية الفريد هذا في عنصر آمن داخل المعدة، وأن تنفذ تدابير أمنية، إلى أقصى حد ممكن من الناحية التكنولوجية، لكشف التلاعب بالعنصر الآمن أو المعلومات المخزنة فيه، ومن ثم، تعطيل الجهاز إلى حين استعادة المعلومات الأصلية.

ويوصى كيان الإدارة المسؤول عن معرّفات الهوية الفريدة بتنفيذ عملية تحفّز مصنّعي الأجهزة المشروعة المخصص لها معرّفات هوية على الاستخدام الصحيح والآمن لها.

ويوصى بأن تمتثل معرّفات الهوية الفريدة لمبادئ السلامة (يجب أن يكون لدى جميع المصنّعين مديات لمعرّفات هوية مخصصة من الكيان المعين) ومبادئ الأمن المحددة من جانب الصناعة (جميع التدابير المحددة أو توليفة منها لتنفيذ معرّفات الهوية على نحو يكون فيه التلاعب بها غير ممكن)[4].

ويوصى بأن تدعم الحكومات أو الأطر التنظيمية الوطنية العمليات التي تطورها الصناعة لإنفاذ هذه المبادئ.

ويجب أن تكون معرّفات الهوية الفريدة غير قابلة لإعادة البرمجة، حتى أثناء خدمة الصيانة. وقد يؤدي السماح بتغيير معرّفات الهوية بعد عملية التصنيع إلى تقليل أمن معرّف الهوية الفريد، مما يتيح لأطراف أخرى غير مخوَّلة التلاعب به.

---

1 انظر المواصفتان التقنيتان [b-3GPP TS 122.016] و[b-3GPP TS 123.003] لمشروع شراكة الجيل الثالث (3GPP) من أجل الأجهزة التي تمتثل إلى مشروع شراكة الجيل الثالث (3GPP)/والمشروع الثاني لشراكة الجيل الثالث (3GPP2).

2 بالنسبة للأجهزة التي تمتثل إلى مشروع شراكة الجيل الثالث (3GPP)/والمشروع الثاني لشراكة الجيل الثالث (3GPP2)، عند استعمال الهوية الدولية للمعدات المتنقلة (IMEI) كمعرّفات هوية فريدة، يمكن أن يساعد في تحقيق هذا المطلب دعم التحقق من الهوية الدولية للمعدات المتنقلة (IMEI) – الهوية الدولية للاشتراك المتنقل (IMSI)، من شبكة النفاذ الراديوية إلى الشبكة الأساسية.

3 مثلاً، المواصفة التقنية [b-3GPP TS 122.016] في مشروع شراكة الجيل الثالث (3GPP) تنص على عدم تغيير الهوية الدولية للمعدات المتنقلة (IMEI).

4 مثلاً، انظر [b-IMEI-SEC] من أجل الأجهزة المتنقلة المتوافقة مع مشروع شراكة الجيل الثالث (3GPP).

4.8 التعاون الوثيق مع وكالات إنفاذ القانون والوكالات المحلية الأخرى

للحد بشكل فعال من تداول أجهزة المسروقة في السوق، يجب إقامة تعاون وثيق بين الكيانات المسؤولة عن رعاية قواعد البيانات المرجعية وتوفيرها ووكالات الجمارك الوطنية وبين هذه الكيانات في مختلف البلدان وأصحاب المصلحة المعنيين. ويراعي ما يلي:

- بما أن السلطات الجمركية وغيرها من الوكالات الوطنية المخوّلة تؤدي دوراً حاسماً في مراقبة المنتجات المزيَّفة واعتراضها، فمن المهم تزويدها بالأدوات اللازمة للتعرف على الأجهزة المسروقة والمفقودة والمغشوشة وحتى الأجهزة القانونية، مثل قاعدة البيانات المرجعية المركزية؛
- يجب وضع إجراءات للإنفاذ والاتصالات بين المنظمات المختلفة وتشغيلها بشكل كامل. ويمكن أن يشمل ذلك تبادل المعلومات ذات الصلة، مثل قواعد بيانات الأجهزة المتنقلة بما يتماشى مع المعايير الوطنية أو الإقليمية أو الدولية؛
- يمكن مكافحة الاتجار غير المشروع بالأجهزة المتنقلة المسروقة، عن طريق استخدام آليات للاستيقان من هوية أي جهاز فردي للتحقق من أنه الجهاز الأصلي إذا سمحت بذلك القوانين واللوائح المعمول بها في ذلك البلد؛
- قد تختار وكالات إنفاذ القانون، بناءً على الأطر القانونية الوطنية، عدم الحجب الفوري للأجهزة لأغراض التحقيق، من أجل تحديد منشأ الأجهزة المسروقة المباعة في السوق، على الرغم من أنه يجب إعطاء الأفضلية لحجب جميع الأجهزة في أسرع وقت ممكن ما لم تكن هناك أسباب مناسبة واستثنائية لعدم القيام بذلك في حالات بعينها.

ويوصى بوجود استراتيجية رائدة رفيعة المستوى صادرة عن الجهات الحكومية العليا لقيادة التحالفات ومجموعة شاملة من التدابير، من أجل تسهيل الالتزامات وتنفيذ الأنشطة من مختلف القطاعات والسلطات المنفصلة عن مجال الصناعة (مثل إنفاذ القانون والجمارك والتجارة).

5.8 أدوات للتحقق من حالة الأجهزة المتنقلة

من اللازم توفير أداة عامة للمستهلكين وأصحاب المصلحة الآخرين للتحقق من حالة الأجهزة المتنقلة. ويجب أن يكون المستهلكون وأصحاب المصلحة الآخرون قادرين على التحقق، ويا حبذا باستخدام الانترنت، مما إذا كانت أجهزة معينة موسومة بأنها مسروقة أو مفقودة.

ويوصى بإدراج الكيان المسؤول عن حجب الجهاز في نتيجة التحقق من الجهاز (بما في ذلك البلد الذي نُفّذ فيه الحجب) لتمكين المستهلك من تجنب شراء أجهزة مسروقة أو امتلاكها وكذلك لمعالجة الشكاوى في حالة وجود حجب غير صحيح أو من طرف ثالث من جراء جهاز مستنسخ له نفس معرّف الهوية. وهذه الأداة مهمة أيضاً بالنسبة للمستهلك لإجراء التحقق قبل الشراء.

ويوصى بأن يجري تجار التجزئة والكيانات المعنية بتداول الأجهزة عمليات تحقق على الأجهزة التي في حوزتهم لضمان عدم وجود بلاغات عن فقدان هذه الأجهزة أو سرقتها أو عن معرّف هوية فريد مستنسخ. وينبغي الاحتفاظ بالسجلات لإثبات إيلاء العناية الواجبة للحد من إمكانية تجارة الأجهزة المبلغ عن فقدانها أو سرقتها أو المحتوية على معرّفات هوية فريدة مستنسخة.

6.8 دعم الأطر القانونية والتنظيمية الوطنية السارية

يوصى بوضع آليات لتحديد الأجهزة المفقودة والمسروقة وحجبها، وأيضاً الأجهزة ذات معرّفات الهوية الفريدة المتلاعب بها في الشبكة المتنقلة، بحيث يتم توفير قدرة من الناحية التقنية للقيام بذلك. وينبغي التحقق من ذلك مع مشغلي الشبكات المتنقلة المحلية.

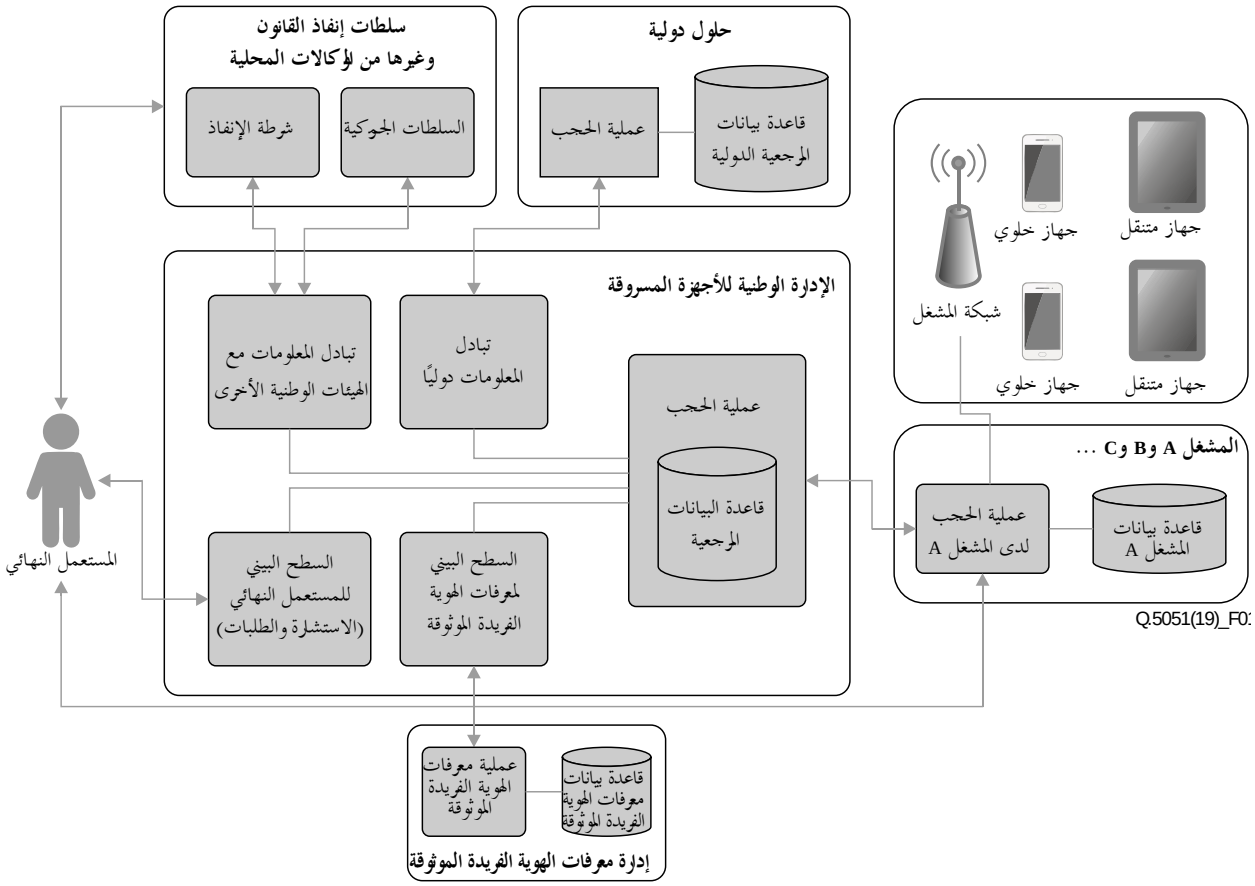
وقبل تنفيذ أي إجراءات تقييدية ضد الأجهزة المسروقة ذات معرّفات الهوية الفريدة المتلاعب بها والمستنسخة، يوصى بالحصول على دعم من الإطار القانوني والتنظيمي الوطني الساري، بما يشمل:

- تقييد النفاذ إلى الشبكة باستعمال الأجهزة المسروقة على الشبكات المتنقلة، سواء المبلغ عنها وطنياً أو في بلد آخر؛
- تقييد النفاذ إلى الشبكة باستعمال الأجهزة المتلاعب بمعرّفات هويتها على الشبكات المتنقلة؛
- تقييد التلاعب بمعرّفات الهوية الفريدة للأجهزة المتنقلة، والآثار الناجمة عن ذلك؛
- وضع السلطات والمستهلكين وقنوات البيع للحلول اللازمة للتمييز بين الأجهزة المعتمدة والمسروقة المتلاعب بها؛
- وجود سلطة مسؤولة عن إنفاذ الإجراءات أعلاه.

وعند النظر في هذه المتطلبات، ينبغي الاحتكام إلى التشريعات الوطنية والأطر التنظيمية القائمة التي قد تعالج بالفعل الجوانب المتناولة.

9 الإطار المرجعي

استناداً إلى متطلبات الإطار المبينة في الفقرة 8، يرد في الشكل 1 رسم بياني للإطار المرجعي المقترح من أجل مكافحة السرقة واستعمال الأجهزة المتنقلة المسروقة. ويجدر بالذكر عدم تطلُّب جميع العناصر الوظيفية الموضحة في الشكل 1، وأن كل بلد يمكنه تنفيذ العناصر وفق احتياجاته.



الشكل 1 – الإطار العام المقترح

ينبغي أن تعمل معاً مجموعة متنوعة من الأنشطة وأنظمة المعلومات، التي تشغلها منظمات مختلفة، للتحكم في المعلومات الهامة وإعدادها بغية تحديد الأجهزة المتنقلة المفقودة والمسروقة وذات معرّفات الهوية غير الصالحة ومكافحة استعمالها.

وينبغي للمستهلك وأصحاب المصلحة الآخرين أن يكونوا قادرين على التحقق مما إذا كان جهاز معين موسوم بتقييد (سرقة أو فقد أو معرّف غير صالح).

ويمكن تقديم طلب حجب جهاز مسروق من خلال أصحاب المصلحة المختلفين (المستهلك أو وكالات إنفاذ القانون أو مشغل الخدمات المتنقلة أو من خلال تقديم الطلب بشكل مباشر إلى النظام المركزي). وبغض النظر عن مكان تقديم طلب حجب الأجهزة قيد الاستعمال، ينبغي اتخاذ الإجراءات من أجل التحقق من هوية المستعمل، وكذلك ملكية الجهاز. أما بالنسبة إلى الأجهزة التي لم تبع إلى المستهلك، مثل الأجهزة المسروقة أثناء النقل العابر والمسروقة من منافذ البيع بالتجزئة وما إلى ذلك، ينبغي أن يكون طلب حجب الجهاز مشفوعاً ببلاغ قانوني.

وبغية الحد من تداول الأجهزة المسروقة في السوق، ينبغي للوكالات الوطنية المعنية الأخرى (مثل وكالات إنفاذ القانون ووكالات الجمارك) أن تتمتع بالقدرة على التحقق من حالة الجهاز باستعمال جميع قواعد البيانات والموارد المرجعية المتاحة.

وتبادل المعلومات مع الكيانات الدولية هو أيضاً أمر بالغ الأهمية ويمكن إنجازه على أساس ثنائي أو باستعمال قاعدة بيانات مرجعية عالمية.

وينبغي لجميع المشغلين تحقيق التزامن مع قاعدة بيانات مرجعية وطنية أو عالمية من أجل ضمان الحجب الفعّال للأجهزة المسروقة على الشبكات المتنقلة للبلد.

ولا بد من دمج إدارة معرّفات الهوية الفريدة الموثوقة في عملية حجب الأجهزة المتنقلة المسروقة، لأنه من الممكن التلاعب بمعرّفات الهوية الفريدة لبعض الأجهزة من أجل تجاوز عملية الحجب.

ويجب تنفيذ عملية لتحديد الأجهزة المتنقلة ذات معرّفات الهوية غير الصالحة ومراقبتها في الشبكات، والتي قد تكون نتيجة للتلاعب بجهاز مسروق بعد حجبه.

10 الميزات المرغوبة

ينبغي للبلدان عند تطبيق أي حل لمكافحة استعمال الأجهزة المتنقلة المسروقة أن تراعي الميزات المرغوبة الواردة في الفقرات التالية.

1.10 قاعدة بيانات مرجعية عالمية للأجهزة المفقودة والمسروقة

بما أن الأجهزة المحجوبة يمكن نقلها وحتى بيعها إلى المستهلكين في مختلف البلدان، يُوصى باستعمال قاعدة بيانات مرجعية عالمية من أجل تبادل معرّفات هوية الأجهزة المفقودة والمسروقة وحجبها لوضع قائمة سوداء بالأجهزة المسروقة في نقطة معلومات واحدة تسهّل التبادل وتقلل المهلة الزمنية اللازمة للحجب.

ويُوصى بمنع توصيل جميع الأجهزة ذات معرّفات الهوية الموجودة في قاعدة البيانات المرجعية العالمية هذه بالشبكات المحلية بغض النظر عن حجم المشغل، بيد أنه يمكن النظر في نُهج بديلة بحسب البيئة الخاصة بكل تنفيذ (مثل معالجة عيوب معرّفات الهوية الفريدة النشيطة إزاء قاعدة البيانات المرجعية العالمية).

ويلزم أن تكون قاعدة البيانات المرجعية العالمية متاحة لسلطات إنفاذ القانون وغيرها من الوكالات الحكومية من أجل التبليغ عن مجموعات من معرّفات الهوية والاستفسار بشأنها لتسهيل الإجراءات القانونية التي تتخذها هذه السلطات والوكالات من أجل محاربة سرقة الأجهزة المتنقلة.

ويُوصى بالتحقق من المعلومات التي تقدم إلى قاعدة البيانات العالمية لأغراض الدقة فيما يخص الأجهزة يتم الإبلاغ عن سرقتها. ولا ينبغي تقديم قوائم الأجهزة المسروقة التي تقوم بتجميعها الأطراف المذكورة أعلاه كي تُدرج في قاعدة بيانات الأجهزة المسروقة تلك إلا بعد إجراء هذا التحقق.

وينبغي إتاحة قاعدة البيانات العالمية تلك لجميع أصحاب المصلحة في أي مكان في العالم من أجل التحقق من الإبلاغ عن سرقة جهاز ما من عدمه. وينبغي أن يكون النفاذ إلى قاعدة البيانات متاحاً على مستوى النظام، للأطراف التي يمكنها حجب الأجهزة المسروقة، وعلى مستوى المستهلك، كي يتسنى للمستهلكين من أي بلد التحقق مما إذا تم الإبلاغ عن سرقة الجهاز من عدمه.

وينبغي أن توفر قاعدة البيانات العالمية معلومات مناسبة إذا كانت هذه المعلومات متوفرة (مثل خصائص الجهاز والبلد الذي سُرق فيه الجهاز وتاريخ وقوع السرقة وما إلى ذلك). وفي حال العثور على معرّفات هوية لأجهزة مسروقة في بلدان متعددة، ينبغي لقاعدة البيانات العالمية أن تذكر هذه المعلومات في نتائجها.

وينبغي تنفيذ الإجراءات بطريقة تتيح للمشاركين في قاعدة البيانات العالمية معالجة الحجب غير المقصود (مثل الحجب الخاطئ والحجب المتعلق بمعرّفات هوية الأجهزة المستنسخة أو المزيفة).

2.10 الإجراءات الخاصة بالمؤسسات التي تبيع الأجهزة المفقودة أو المسروقة أو المغشوشة

يُوصى بأن تنظر البلدان في إطار يحدد مسؤوليات نقاط البيع بحيث لا تقوم إلا بطرح الأجهزة المعتمدة النوع للبيع، وعواقب طرح الأجهزة المسروقة أو الأجهزة ذات معرّفات الهوية المتلاعب بها. وسيزود ذلك وكالات إنفاذ القانون بدعم قانوني من أجل محاربة بيع هذه الأجهزة والطلب عليها.

ويمكن أن تُدرج معرّفات هوية الأجهزة المستوردة والمباعة قانونياً في قاعدة البيانات المرجعية الوطنية. ويمكن لقاعدة البيانات هذه أن تساعد في طائفة من الإجراءات والأنشطة الوطنية الخاصة بالإنفاذ مثل الاستيراد والبيع والاستعمال في الشبكات والإجراءات التي تتخذها سلطة إنفاذ القانون وما إلى ذلك.

وبالتالي، يمكن أن يساعد ذلك وكالات إنفاذ القانون في النفاذ إلى قاعدة البيانات هذه الخاصة بالأجهزة المعتمدة من أجل اتخاذ الإجراءات إزاء المؤسسات التي تطرح للعامة أجهزة مسروقة أو متلاعب بها أو مستنسخة، أو حتى في التعرف على المنتجات المستوردة بشكل غير قانوني واعتراضها.

التذييل I

النهج الذي تطبقه رابطة شركات تشغيل الاتصالات المتنقلة لمحاربة سرقة الأجهزة المتنقلة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

كما هو الحال في عدد متنامٍ من الدول، يوفر المشغلون للمستهلكين إمكانية التبليغ عن جهاز متنقل بوصفه مفقوداً أو مسروقاً. ويمكن للمشغل بعد ذلك أن يحدد معرّف الهوية الفريد للجهاز أي IMEI، بعدها يمكن لمشغل الشبكة المتنقلة حجب الهاتف من النفاذ إلى شبكته المتنقلة. ويطلق على ذلك إدراج الهوية IMEI الخاصة بالجهاز في القائمة السوداء[5].

وكمثال على استعمال قاعدة بيانات عالمية، في أوساط مشغلي الخدمات المتنقلة تُقدم الهويات الدولية للمعدات المتنقلة المدرجة في القائمة السوداء إلى قاعدة البيانات العالمية لرابطة شركات تشغيل الاتصالات المتنقلة الخاصة بالهوية الدولية للمعدات المتنقلة مما يتيح للمشغلين تبادل البيانات وحجب الأجهزة على شبكات متعددة وطنياً ودولياً.

وتحتفظ قاعدة بيانات الرابطة GSMA للهويات الدولية للمعدات المتنقلة بقائمة سوداء عالمية مجمّعة من البيانات التي يوفرها المشغلون المشاركون. وتوفر الرابطة معلومات القائمة السوداء على مدار الساعة طيلة أيام الأسبوع للمشغلين الذين أقاموا توصيلات بقاعدة بيانات الهويات الدولية للمعدات المتنقلة لأغراض التنزيل والاستعمال في شبكاتهم من أجل حجب الأجهزة. ويختار المشغلون المشاركون قائمة مشغل ما ويستخرجون منها بيانات القائمة السوداء وهذا ما يحدد الدرجة التي تم التوصل إليها فيما يتعلق بمستوى تبادل البيانات.

ومن غير الواضح في كثير من الأحيان بالنسبة إلى المشتركين الذين يقومون بإبلاغ مورد الخدمة عن فقدان جهاز ما عما إذا كان هذا الجهاز مفقوداً أو مسروقاً، ولذا لا يوجد بشكل عام تمييز بين الحالتين. وإذا عثر المالك على الجهاز وبلّغ مورد الخدمة، يمكن إزالة الحجب عن الجهاز وإزالة الهوية الدولية للمعدات المتنقلة من قاعدة بيانات الهوية الدولية للمعدات المتنقلة. وترسل بعد ذلك الرابطة GSMA تعليمات للحذف من القائمة السوداء إلى المشغلين المعنيين الذين قاموا بتنزيل السجل الأصلي للقائمة السوداء.

ونظراً إلى طبيعة قاعدة البيانات العالمية هذه والتزام أصحاب المصلحة المختلفين في السوق بمنع سرقة الأجهزة، أنشأت الرابطة GSMA مرفقاً للسماح بالتحقق من حالة الهويات الدولية للمعدات المتنقلة. ويُعرف هذه النظام باسم "التحقق من الأجهزة" ويتيح تبادل البيانات ومعلومات حالة الجهاز مع الشركاء المعتمدين، بما في ذلك شركات البيع بالتجزئة وشركات التأمين وشركات إعادة التدوير ووكالات إنفاذ القانون.

وبفضل هذا النظام يمكن لأصحاب المصلحة المعنيين أن يكتشفوا ما إذا كان جهاز ما قد تم التبليغ عن فقده أو سرقته، فضلاً عن توفير معلومات عن سنوات من تاريخ الجهاز ومعلومات عن طراز الجهاز وإمكاناته. وينتج عن هذا النوع من التحقق فوائد عديدة، منها ما يلي: (أ) مساعدة الموزعين على التعرف على تحديد الأجهزة المسروقة والتخلص منها قبل دخولها في سلاسل التوريد؛ (ب) التأكد من الطراز الحقيقي للجهاز لأغراض الاستيقان والمساعدة في تحديد قيمة الجهاز؛ (ج) الثني عن سرقة الأجهزة عن طريق التقليل من قيمة الأجهزة المسروقة (د) التأكيد لمشغل الشبكة بأن الجهاز المبلغ عنه مفقود أو مسروق مما يساعد على إعادة الجهاز إلى المالك الشرعي.

وإضافة إلى مشغلي الشبكات، يمكن للعديد من المنظمات الأخرى في النظام الإيكولوجي للأجهزة المتنقلة استعمال خدمة التحقق من الأجهزة، بما في ذلك (أ) هيئات إعادة تدوير الأجهزة وبيعها والاتجار بها التي تستعمل البيانات للتقليل من احتمال دخول الأجهزة المبلغ عن سرقتها أو فقدها في مسار إعادة التدوير أو التوزيع؛ (ب) شركات التأمين التي تعتمد على قاعدة البيانات

5 انظر المرجع [b-GSMA-IMEI-Blklst].

من أجل التقليل من طلبات التأمين الكاذبة أو المبالغ فيها بخصوص أجهزة مفقودة/مسروقة؛ (ج) وكالات إنفاذ القانون التي تستعمل الخدمة من أجل التعرف على البضائع المسروقة أو المفقودة والمساعدة في التحقيق بشأنها و/أو إعادتها.[6]

ويمكن توفير النفاذ إلى طائفة من أصحاب المصلحة الإضافيين، بمن فيهم المستهلكون، للاستفسار على معرّف هوية وحيد في قاعدة البيانات العالمية للهوية الدولية للمعدات المتنقلة، وذلك من خلال عروض الخدمات المقدمة من كيانات مثل السلطات الوطنية والتي تتضمن اللغة المحلية ومنافذ تسمح بالاطلاع على الهويات الدولية للمعدات المتنقلة. وحالياً، لا يتاح النفاذ لتقديم مدخلات إلى القائمة السوداء و/أو إزالة المعرّفات من القائمة السوداء إلا إلى مشغلي الشبكات الذين يمكنهم تحديد وتوثيق بيانات الهوية الدولية للمعدات المتنقلة لزبائنهم على نحو لا لبس فيه، والحفاظ بالتالي على سلامة القائمة السوداء. ويؤخذ بعين الاعتبار توسيع النفاذ المناسب إلى القائمة السوداء ليشمل أطراف أخرى، من قبيل مصنعي الأجهزة وتجار البيع بالتجزئة وغيرهم، الذين يمكن توثيق وضمان حجب الهوية الدولية للمعدات المتنقلة.

وتوفر الأنظمة ذات الصلة المبينة أعلاه (قاعدة بيانات الرابطة GSMA الخاصة بالهويات الدولية للمعدات المتنقلة ونظام التحقق من الأجهزة (IMEI Device Check)) إلى أصحاب المصلحة مجموعة من المزايا بالمقارنة مع قواعد البيانات الوطنية التي تفضي إلى التشتت، بيد أنه يمكن بناؤها نتيجةً للجهود الثنائية أو متعددة الأطراف من أجل تبادل معرّفات الهوية التي تم التبليغ عن فقدها أو سرقتها، وحجبها. ويمكن أن تشكل هذه المزايا ما يلي: (أ) مهلة زمنية أقل من أجل التنفيذ والتوليف الدقيق؛ (ب) قدراً أقل من تكاليف النفقات الرأسمالية (CAPEX) والنفقات التشغيلية (OPEX)؛ (ج) قدراً أقل من التعقيد ومزيداً من الفعالية (نقطة تبادل مشتركة واحدة عوضاً عن وجود مصادر ومقاصد عديدة)؛ (د) قدراً أقل من ازدواجية المعلومات. وتستند هذه البنود إلى الخصائص التالية للأنظمة المشار إليها: (أ) التقسيم إلى وحدات نمطية؛ (ب) عدم وجود رسوم توصيل للمشغلين/الحكومات؛ (ج) قاعدة بيانات الهوية الدولية للمعدات المتنقلة هي منصة تكنولوجيا مكتملة وثابتة موجودة منذ عام 1996.

6 انظر [b-GSMA-IMEI-DevChk].

بيبليوغرافيا

[b-ITU-T X.Sup.19] ITU-T X-series Recommendations – Supplement 19 (2013), Supplement on security aspects of smartphones.

[b-IMEI-SEC] GSMA (2016), *IMEI Security Design Principles. Enabling stolen mobile device blocking. V4.0.* <https://imeidb.gsma.com/imei/resources/documents/IMEI-Security-Technical-Design-Principles-v4.pdf>

[b-3GPP TS 122.016] ETSI TS 122 016 V3.1.0 (2000-01), *Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); International Mobile station Equipment Identities (IMEI) (3G TS 22.016 version 3.1.0 Release 1999).*

[b-3GPP TS 23.003] ETSI TS 123 003 V10.5.0 (2012-04), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003 version 10.5.0 Release 10).*

[b-GSMA] GSM Association, Official Document SG.24 (2016), *Anti-Theft Device Feature Requirements v3.0.*

[b-GSMA-IMEI-Blklst] GSMA Services, *IMEI Blacklisting*. <https://www.gsma.com/services/gsma-imei/imei-blacklisting/> (last accessed 13 April 2020)

[b-GSMA-IMEI-DevChk] GSMA Services, *Device Check*. <https://www.gsma.com/services/gsma-imei/about-device-check/> (last accessed 13 April 2020)

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	**التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما**
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2020