

Q.5050

(2019/03)

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

السلسلة Q: التبديل والتشوير، والقياسات والاختبارات
المرتبطة بهما

مكافحة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة والمسروقة

إطار حلول لمكافحة أجهزة تكنولوجيا المعلومات
والاتصالات المزيفة

التوصية ITU-T Q.5050

توصيات السلسلة Q الصادرة عن قطاع تقييس الاتصالات
التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما

Q.3-Q.1	التشوير في الخدمة اليدوية الدولية
Q.59-Q.4	التشغيل الدولي الأوتوماتي وشبه الأوتوماتي
Q.99-Q.60	الوظائف وتدفق المعلومات في خدمات الشبكات الرقمية المتكاملة الخدمات (ISDN)
Q.119-Q.100	البنود المطبقة على الأنظمة المعمارية في قطاع تقييس الاتصالات
Q.499-Q.120	مواصفات أنظمة التشوير رقم 4 و 5 و 6 و R1 و R2
Q.599-Q.500	البدايات الرقمية
Q.699-Q.600	التشغيل البيئي في أنظمة التشوير
Q.799-Q.700	مواصفات نظام التشوير رقم 7
Q.849-Q.800	السطح البيئي Q3
Q.999-Q.850	نظام التشوير الرقمي رقم 1 للمشارك
Q.1099-Q.1000	الشبكات المتنقلة البرية العمومية
Q.1199-Q.1100	التشغيل البيئي مع الأنظمة المتنقلة الساتلية
Q.1699-Q.1200	الشبكية الذكية
Q.1799-Q.1700	متطلبات وبروتوكولات التشوير للأنظمة المتنقلة الدولية-2000
Q.1999-Q.1900	مواصفات التشوير المتعلقة بتحكم في النداء مستقل عن حامل النداء (BICC)
Q.2999-Q.2000	الشبكية ISDN عرضة النطاق
Q.3709-Q.3000	متطلبات وبروتوكولات التشوير لشبكات الجيل التالي
Q.3899-Q.3710	متطلبات وبروتوكولات التشوير
Q.4099-Q.3900	مواصفات الاختبار
Q.5049-Q.5000	متطلبات وبروتوكولات التشوير للأنظمة المتنقلة الدولية-2020
Q.5069-Q.5050	مكافحة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة والمسروقة

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

إطار حلول لمكافحة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة

ملخص

ما برح استخدام معدات تكنولوجيا المعلومات والاتصالات (ICT) يتزايد في الحياة اليومية للناس، في السنوات الأخيرة، ولكن ظهرت أيضاً آثار جانبية غير مستساغة تتعلق بزيادة مبيعات أجهزة تكنولوجيا المعلومات والاتصالات المزيفة وتداولها واستخدامها في السوق.

وجهاز الاتصالات/تكنولوجيا المعلومات والاتصالات المزيف منتج ينتهك انتهاكاً واضحاً العلامات التجارية، وينسخ تصاميم الأجهزة أو البرمجيات، وينتهك حقوق العلامة التجارية أو التعبئة والتغليف للمنتج الأصلي أو الحقيقي، وبصفة عامة، فهو ينتهك المعايير التقنية المنطبقة على الصعيد الوطني و/أو الدولي، والمتطلبات التنظيمية أو عمليات المطابقة، أو اتفاقات ترخيص التصنيع، أو المتطلبات القانونية المنطبقة الأخرى.

ومن بين الأنواع المختلفة من أجهزة تكنولوجيا المعلومات والاتصالات المستخدمة اليوم، أصبحت الهواتف الذكية وغيرها من الأجهزة المتنقلة من بين السلع السائدة والمرغوبة بين سكان العالم، وكان من بين آثارها الجانبية أيضاً أنها أثارت اهتمام السوق السوداء/الموازية العالمية. وينتج عن ذلك عواقب سلبية على أصحاب المصلحة مثل المستخدمين ومشغلي الشبكات ومصنعي الأجهزة الأصلية والتجار والحكومات، بما في ذلك تراجع الحماية الأمنية وجودة الخدمة للمستخدمين وخسائر إيرادات لمجموعة من أصحاب المصلحة.

وبما أن اقتصاد العرض والطلب لأجهزة تكنولوجيا المعلومات والاتصالات المزيفة يُعقّد محاولات معالجة سوق المزيفات العالمية، فلا يمكن لأي حل وحيد أن يحل المشكلة بمفرده، مما يتطلب اتخاذ مجموعة واسعة من التدابير في إطار نهج كلي.

ولذلك، تهدف التوصية ITU-T Q.5050 إلى وصف إطار مرجعي، مع التحديات والمتطلبات الإجمالية التي تنبغي مراعاتها لدى نشر الحلول لمكافحة تداول واستخدام أجهزة تكنولوجيا المعلومات والاتصالات المزيفة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T Q.5050	2019-03-15	11	11.1002/1000/13702

مصطلحات أساسية

مكافحة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة، التزام، مطابقة، تقييم المطابقة، إطار، متطلبات، أمن، معيار، معرفات فريدة.

* للاطلاع على التوصية، الرجاء 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 والتعريف، 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 الكهروتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها. والتقييد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيئي والتطبيق مثلاً). ويعتبر التقييد بهذه التوصية حاصلاً عندما يتم التقييد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقييد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعى 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/>.

© ITU 2019

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

جدول المحتويات

الصفحة

1 مجال التطبيق	1
1 المراجع	2
1 التعاريف	3
1 1.3 المصطلحات المعرّفة في وثائق أخرى	
2 2.3 مصطلحات معرفة في هذه التوصية	
2 المختصرات والأسماء المختصرة	4
3 الاصطلاحات	5
3 الجوانب العامة	6
4 أسس سوق معدات الاتصالات النظامية	7
4 اعتبارات عند نشر حلول لمكافحة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة:	8
4 1.8 كشف أجهزة تكنولوجيا المعلومات والاتصالات المزيفة والتعرف عليها	
5 2.8 تعقب منتجي أجهزة تكنولوجيا المعلومات والاتصالات المزيفة والمتاجرين بها	
5 3.8 سحب أجهزة تكنولوجيا المعلومات والاتصالات المزيفة المستخدمة الآن من السوق	
6 4.8 الحد من استيراد أجهزة تكنولوجيا المعلومات والاتصالات المزيفة الجديدة وتداولها وبيعها في السوق	
6 5.8 التفريق بين أجهزة تكنولوجيا المعلومات والاتصالات الأصلية والمزيفة	
6 6.8 الحد من التأثير على مصنعي أجهزة تكنولوجيا المعلومات والاتصالات المعتمدة	
 7.8 الحد من التأثير على المستخدم النهائي عند النظر في سحب أجهزة تكنولوجيا المعلومات والاتصالات المزيفة	
6 8.8 تثقيف المستهلكين	
7 9.8 تجنب الحواجز التقنية المعوّقة للتجارة (TBTs)	
7 متطلبات الإطار	9
7 1.9 إجراءات التعرف والإنفاذ ضد منتجي ومهربي الأجهزة المزيفة	
7 2.9 التشاور مع دوائر الصناعة ومجموعات المستهلكين	
8 3.9 المعارف الفريدة الموثوقة	
8 4.9 قاعدة البيانات المرجعية المركزية	
8 5.9 نشر نظام تقييم المطابقة	
9 6.9 التعاون الوثيق مع سلطات الجمارك والوكالات المحلية المناسبة	
9 7.9 تبادل المعلومات مع المستخدم النهائي قبل أي إجراء تصحيحي	
9 8.9 دعم الأطر القانونية والتنظيمية الوطنية السارية	

10	9.9	مراجعة المنتجات المستخدمة الآن في السوق
10	10	تُحج حل ممكنة لتكنولوجيا المعلومات والاتصالات المزيفة
10	1.10	حظر استخدام معرفات جهاز غير صحيحة وغير أصلية
11	2.10	إصدار شهادات لأجهزة تكنولوجيا المعلومات والاتصالات ومراقبة السوق
11	3.10	إدارة دورة حياة الجهاز
12	11	الإطار المرجعي
14		الملحق A - حلول الأجهزة المتنقلة
17		التذييل I - الحلول الأخرى لدى دوائر الصناعة
20		بيبلوغرافيا

إطار حلول لمكافحة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة

1 مجال التطبيق

تشمل هذه التوصية الإطار المرجعي مع المتطلبات التي يتعين النظر فيها لدى نشر الحلول لمكافحة تداول واستخدام أجهزة تكنولوجيا المعلومات والاتصالات (ICT) المزيفة.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكّل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبقات 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. لا توجد.

3 التعاريف

1.3 المصطلحات المعرّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرّفة في وثائق أخرى:

1.1.3 تقييم المطابقة [b-ISO/IEC 17000]: هو بيان أن المتطلبات المحددة المتعلقة بالمنتج أو العملية أو النظام أو الشخص أو الجسم قد استوفيت.

2.1.3 مخطط (أو برنامج) تقييم المطابقة [b-ISO/IEC 17000]: هو نظام تقييم مطابقة يتعلق بمواضيع تقييم المطابقة المحددة التي تنطبق عليها نفس المتطلبات المحددة، والقواعد والإجراءات المحددة.

3.1.3 مراقبة السوق [b-EC-Regulation]: هي الأنشطة التي تنفذها السلطات العامة والتدابير التي تتخذها لضمان التزام المنتجات بالمتطلبات المنصوص عليها في التشريعات ذات الصلة وعدم تهديدها للصحة أو السلامة أو أي جانب آخر من جوانب حماية المصلحة العامة.

4.1.3 معيار [b-WTO-TBT]: هو وثيقة توافق عليها هيئة معترف بها، تقدم، للاستخدام الشائع والمتكرر، قواعد أو مبادئ توجيهية أو خصائص للمنتجات أو للعمليات وأساليب الإنتاج ذات الصلة، دون أن يكون الالتزام بها إلزامياً. ويجوز أن تتضمن أيضاً أو تتعامل حصرياً مع مصطلحات أو متطلبات رموز أو عبوات أو وسوم أو علامات حسبما تنطبق على منتج أو عملية أو أسلوب إنتاج.

5.1.3 المراقبة [b-ISO/IEC 17000]: هي التكرار المنتظم لأنشطة تقييم المطابقة كأساس للحفاظ على صحة بيان المطابقة.

6.1.3 الحواجز التقنية المعوّقة للتجارة (TBT) [b-WTO-TBT]: يهدف اتفاق الحواجز التقنية المعوّقة للتجارة لدى منظمة التجارة العالمية (WTO) إلى ضمان أن تكون اللوائح والمعايير وإجراءات تقييم المطابقة التقنية غير تمييزية وألا تضع عقبات غير ضرورية أمام التجارة.

7.1.3 اللائحة التقنية [b-WTO-TBT]: هي الوثيقة التي تنص على خصائص المنتج أو العمليات وأساليب الإنتاج المرتبطة به، بما في ذلك الأحكام الإدارية المعمول بها التي يكون الالتزام بها إلزامياً. ويجوز أن تتضمن أيضاً أو تتعامل حصرياً مع مصطلحات أو متطلبات رموز أو عبوات أو وسوم أو علامات حسبما تنطبق على منتج أو عملية أو أسلوب إنتاج.

8.1.3 السوق الموازية [b-Gartner]: هي استيراد وبيع الأجهزة خارج القنوات التجارية العادية على النحو المحدد من الشركة المصنعة الأصلية أو الحكومة المعنية، مما يؤدي إلى إنشاء سوق موازية لقنوات التوزيع المعتمدة.

2.3 مصطلحات معرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 جهاز تكنولوجيا المعلومات والاتصالات المزيف: هو جهاز تكنولوجيا المعلومات والاتصالات (ICT) الذي ينتهك انتهاكاً واضحاً العلامات التجارية، وينسخ تصاميم الأجهزة أو البرمجيات، وينتهك حقوق العلامة التجارية أو التعبئة والتغليف للمنتج الأصلي أو الحقيقي، وبصفة عامة، فهو ينتهك المعايير التقنية المنطبقة على الصعيد الوطني و/أو الدولي، والمتطلبات التنظيمية أو عمليات المطابقة، أو اتفاقات ترخيص التصنيع، أو المتطلبات القانونية المنطبقة الأخرى.

2.2.3 جهاز تكنولوجيا المعلومات والاتصالات المغشوش: هو جهاز تكنولوجيا المعلومات والاتصالات (ICT) يتضمن مكونات أو برمجيات أو معرفات هوية فريدة أو منتجات تحميها حقوق الملكية الفكرية أو علامات تجارية تعرضت للتغيير مبدئياً أو فعلياً دون موافقة صريحة من الجهة المصنعة أو ممثلها القانوني.

3.2.3 المعرف الفريد: معرف يرتبط بجهاز واحد ويهدف إلى الانفراد بتعريفه.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

CAS	مخطط تقييم المطابقة (Conformity Assessment Scheme)؛
DevID	معرف الجهاز (Device Identifier)
DIRBS	نظام التعرف على الجهاز وتسجيله وحجبه (Device Identification, Registration, and Blocking System)
EAP	بروتوكول الاستيقان القابل للتوسعة (Extensible Authentication Protocol)
EIR	سجل هوية المعدات (Equipment Identity Register)
ICT	تكنولوجيا المعلومات والاتصالات (Information and Communications Technology)
IMEI	الهوية الدولية للمعدات المتنقلة (International Mobile Equipment Identity)
IoT	إنترنت الأشياء (Internet of Things)
IPR	حقوق الملكية الفكرية (Intellectual Property Rights)
IVR	رد صوتي تفاعلي (Interactive Voice Response)
PCB	لوحة دائرة مطبوعة (Printed Circuit Board)
SIM	وحدة تعريف هوية المشترك (Subscriber Identification Module)
TAC	شفرة توزيع النمط (Type Allocation Code)
TBT	حاجز تقني معوّق للتجارة (Technical Barrier to Trade)

بيئة تنفيذ موثوقة (Trusted Execution Environment)	TEE
وحدة منصة موثوقة (Trusted Platform Module)	TPM
الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (Trade-Related Aspects of Intellectual Property Rights)	TRIPS

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) وكلمة "ينبغي" تدل 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 يفعله مشغل الشبكة/مقدم الخدمة بشكل اختياري. بل إن المصنع يمكنه إدراج هذا الخيار وزعم المطابقة مع هذه التوصية في نفس الوقت.

6 الجوانب العامة

ما برح الاستخدام الإيجابي لأجهزة تكنولوجيا المعلومات والاتصالات يتزايد في الحياة اليومية للناس، في السنوات الأخيرة، ولكن ظهرت أيضاً آثار جانبية غير مستساغة تتعلق بزيادة مبيعات أجهزة تكنولوجيا المعلومات والاتصالات المزيفة وتداولها واستخدامها في السوق. وقد أدى ذلك إلى عواقب سلبية على أصحاب المصلحة المتعددين مثل المستخدمين ومشغلي الشبكات ومصنعي الأجهزة الأصلية والتجار والحكومات، بما في ذلك تراجع الحماية الأمنية وجودة الخدمة للمستخدمين وخسائر إيرادات مجموعة من أصحاب المصلحة.

ومن المعلوم أن اقتصاد العرض والطلب بشأن أجهزة الاتصالات/تكنولوجيا المعلومات والاتصالات المزيفة يعقد محاولات التصدي للسوق السوداء/الموازية العالمية، وأن ما من حل واحد لمكافحة التزييف يمكن أن يكون دواءً لكل داء. وتقتصر التوصية الحالية إطاراً يتألف من مجموعة واسعة من التدابير التي يمكن اتخاذها وتطبيقها في إطار نهج شامل لمعالجة هذه المشكلة. وينبغي أيضاً التصدي لمصدر المنتجات المزيفة قدر الإمكان ضمن الأسواق التي تصنع فيها وتصدر منها بمساعدة البلدان التي تباع فيها.

وقد يصعب بوجه خاص التفريق بين أجهزة تكنولوجيا المعلومات والاتصالات الأصلية والمزيفة على أي شخص يعاين منتج ما أو يفحصه لأن أهداف التزييف تتمثل في تليفق منتجات مشابهة تماماً للأجهزة الأصلية من خلال تقديم وثائق أصلية مزورة أو مسروقة، بما في ذلك أحياناً عتاد مأخوذ من المنتج الأصلي أو ملحقاته وحتى نسخ برمجيات مشروعة أو معرفات فريدة، وكل ذلك لإعاقة جميع أصحاب المصلحة عن تحديد الهوية. ومن الأهمية بمكان أخذ هذه العوامل وغيرها بعين الاعتبار عند تنفيذ الحلول، لتجنب خلق مشاكل للمستخدمين والمصنعين الأصليين أكثر من تلك التي سعت الحلول لحلها.

ومن بين الأنواع المختلفة لأجهزة تكنولوجيا المعلومات والاتصالات المستخدمة اليوم، أصبحت الهواتف الذكية وغيرها من الأجهزة المتنقلة من بين السلع السائدة والمرغوبة بين سكان العالم، وكان من بين آثارها الجانبية أيضاً أنها أثارت اهتمام السوق السوداء/الموازية العالمية. ورداً على مشكلة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة، تبنت بعض البلدان تدابير ونشرت حلولاً ناجحة لردع تداول أجهزة تكنولوجيا المعلومات والاتصالات المزيفة واستخدامها في الوقت الذي تواجه فيه الحكومات في بلدان أخرى صعوبة وغموض بشأن أفضل الاستراتيجيات التي يجب اعتمادها.

وفي مسعى للتصدي لاستخدام أجهزة تكنولوجيا المعلومات والاتصالات المزيفة، تتخلل العديد من الحلول المعتمدة بعض أوجه التشابه، مثل الاعتماد على معرفات الأجهزة الفريدة، وعلى مساعدة نظام تقييم المطابقة. وعلى وسائل لمنع نفاذ هذه الأجهزة المزورة إلى الشبكة (على النحو المقترح للأجهزة المتنقلة في الملحق A).

بيد أن حكومات متنوعة في جميع أنحاء العالم لا تزال تواجه تحديات في مكافحة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة لأسباب مختلفة تشمل الجوانب التقنية، وجهود المزيّفين لتفادي وتجنب الكشف، والاستحسان الصريح لهذه المنتجات بمعنى أن المستهلكين يتخذون قراراً متعمداً بشراء المنتجات المزيفة.

ولذلك، ينبغي للبلدان التي تختار مكافحة تكنولوجيا المعلومات والاتصالات المزيفة أن تنظر في اتباع نهج وحلول تكنولوجية شاملة متعددة الوكالات/أصحاب المصلحة تنفّذ في بلدان أخرى منخرطة بالفعل في هذه القضية، للحصول على إرشادات وأمثلة بشأن أفضل الممارسات في هذا الصدد.

7 أسس سوق معدات الاتصالات النظامية

تتعدد العوامل الكامنة وراء إنشاء سوق نظامية لمنتجات وخدمات الاتصالات. ومن المتطلبات الأساسية لذلك، وضع متطلبات تقنية مشددة للمنتجات التي تدخل السوق. وتتناول هذه المتطلبات، من بين أمور أخرى، سلامة الأفراد، أي سلامة مجتمع المستخدمين وموظفي مقدم خدمة الشبكة على السواء، وإنشاء بيئة خالية من التداخل لخدمات الاتصالات.

وللخدمات الخالية من التداخل - اللاسلكية والسلكية - دور في التنمية الاقتصادية للمجتمع حيث تتطلب المشاركة في الاقتصاد الرقمي العالمي منصات اتصالات قوية وآمنة ويمكن الاعتماد عليها ليدب النشاط الاقتصادي عبرها. وعلاوة على ذلك، فإن نظام النفاذ إلى الأسواق حسن التعريف والإدارة وغير التمييزي والشفاف، يلهم الثقة في موردي المعدات ومقدمي الخدمات والأشخاص بشكل عام. ويشكل هذا النظام المدعوم بإطار تشريعي وتنظيمي ملائم لبنة أساسية في تقديم الجودة المطلوبة للتوصيلية الوطنية والدولية الحرجة للمشاركة في الاقتصاد الرقمي العالمي. وهو، في الواقع، يعبر حقاً عن أولويات وقيم المجتمع [b-ITU-D-CI-Guidelines].

8 اعتبارات عند نشر حلول لمكافحة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة:

تتعدد التحديات التي يواجهها أصحاب المصلحة عند تنفيذ حلول للتعامل مع أجهزة تكنولوجيا المعلومات والاتصالات المزيفة:

1.8 كشف أجهزة تكنولوجيا المعلومات والاتصالات المزيفة والتعرف عليها

يتمثل أحد أهداف المزيّفين في تمكين بيع منتجاتهم في الأسواق حول العالم. ومن حيث الشكل والمظهر، ونسخ المعارف الفريدة، والبرمجيات وحتى مكونات الأجهزة الداخلية لأجهزة تكنولوجيا المعلومات والاتصالات، سيبدل المزيّفون قصارى جهدهم لجعل المنتج أقرب ما يمكن إلى المنتج الأصلي.

ويطرح ذلك بعض التحديات. فعلى سبيل المثال، جميع المعارف التي تستحدثها الشركات المصنعة الأصلية للسلع يمكن أن يسيء المزيّفون استخدامها من أجل تحقيق أهدافهم في إيهام المستهلكين والسلطات بأن منتجاتهم أصلي. وأي آلية تُعرف وما يحيط بها من إجراءات أمنية يمكن أن تصبح هدفاً للمزيّفين والمجرمين. وكثيراً ما تحزّب شعارات وأيقونات اعتماد النوع وكذلك معرفاته الإلكترونية على نحو متعمد أو حتى تفرّغ لتبرمج ذاتياً في الأسواق المحلية وللتهرب من تفتيش الجمارك وسلطات إنفاذ القانون عند الحدود.

[b-ITU-T TR-Counterfeit]

وجميع المعارف التي تستحدثها الشركات المصنعة الأصلية للسلع يمكن أن يتلاعب بها المزيّفون من أجل تحقيق أهدافهم في إيهام المستهلكين والسلطات بأن منتجاتهم أصلي. وهذه مشكلة تصادف في العديد من الصناعات، وليست حكراً على تكنولوجيا المعلومات والاتصالات. وينبغي أن يضع القارئ في الاعتبار أن أي آلية تُعرف وما يحيط بها من إجراءات أمنية ستصبح هدفاً للمزيّفين والمجرمين. [b-ITU-T TR-Counterfeit]

فعلى سبيل المثال، تتمثل إحدى الممارسات الشائعة للمزيّفين في التلاعب بالمعارف الفريدة التي تستخدمها بعض الأجهزة للاستيقان على الشبكة بطريقة تتعرف بها الشبكة على أجهزة تكنولوجيا المعلومات والاتصالات المزيفة باعتبارها معدات أصلية. وهناك ممارسة أخرى تتمثل في اعتراض الأجهزة الأصلية والتلاعب ببرمجياتها بحيث تبدو كأنها نسخة مطورة (وأكثر تكلفة) أو حتى الاستعاضة عن قطع أصلية داخلية فيها، مثل البطاريات، بنسخ مزيفة من أجل بيع القطع الأصلية في السوق.

وكثيراً ما تحزّب شعارات وأيقونات اعتماد النوع وكذلك معرفاته الإلكترونية على نحو متعمد للتهرب من تفتيش الجمارك وسلطات إنفاذ القانون عند الحدود. ويخلق ذلك إشكالات عملية للمصنعين والمستهلكين والجمارك وموظفي إنفاذ القانون الذين يصعب عليهم تمييز العلامات المعرّفة المزيفة عن الأصلية، حتى قبل النظر في المنتج نفسه.

2.8 تعقب منتجي أجهزة تكنولوجيا المعلومات والاتصالات المزيفة والمتاجرين بها

عند التعرف على جهاز غير نظامي، ينبغي للجهات المعنية أن تتبع اقتصادات منشأ الأجهزة غير القانونية ومنتجها والمتاجرين بها وإزالتهم من السوق [b-OECD].

وبدون إجراءات فعالة للتعرف والإنفاذ ضد المنتجين والمتاجرين في اقتصادات المصدر، قد لا تجدي الإجراءات المتخذة في اقتصادات المقصد نفعاً.

3.8 سحب أجهزة تكنولوجيا المعلومات والاتصالات المزيفة المستخدمة الآن من السوق

تعتمد مراقبة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة بعد انتشارها في السوق على فرص اتخاذ إجراءات بشأنها. ويمكن أن تتمثل الإجراءات المحتملة في '1' الكشف والتحقق، مادياً أو عن بعد، بالمقارنة مع خصائص المنتج الأصلي، و/أو '2' كف استخدامها و/أو '3' مصادرتها.

وتنطوي هذه الفرص والإجراءات على عدة تحديات:

- للتحقق من جهاز مادياً، تسنح بعض الفرص: خلال مناسبة صيانة، أو حدث مراقبة السوق، أو في بعض الحالات حيث يحق للسلطة القانونية فحص الجهاز. ويتمثل التحدي هنا في إنشاء قاعدة المعرفة المطلوبة واهتمام الوكالات بالقيام بهذه المهام.
- ويمكن إجراء التحقق بطريقة منطقية أو عن بُعد، ومثال ذلك التحقق بأساليب بديلة من المعرفات الفريدة وبصمات المنتج أثناء نوع ما من تسجيل النظام عبر الإنترنت، ولكن ذلك يتطلب عموماً توصيلاً بالإنترنت وهو ما قد يصعب في البيئات البعيدة أو الريفية، لا سيما في البلدان النامية في العالم. وعلى الرغم من أن العمليات الإلكترونية ينبغي أن تشارك في الأمر، لا بد من القدرة على مقارنة الخصائص المادية مع المعلومات الموجودة في قواعد بيانات المنتج.
- وإذا كان الجهاز يستخدم معرفاً فريداً للتسجيل على الشبكة، فيمكن رفض هذا التسجيل لأجهزة تكنولوجيا المعلومات والاتصالات المزيفة من خلال استخدام قاعدة بيانات الأجهزة المجاز تشغيلها في سوق محددة. ويتمثل التحدي في بناء وصيانة نظام التسجيل وقاعدة بيانات، خاصة إذا سبق أن نُشر عدد كبير من الأجهزة بدون هذا النوع من الضوابط.
- وينبغي توخي الحذر لتجنب إساءة استخدام أنظمة التعريف والتسجيل، واحترام حقوق المستهلك وعدم التأثير سلباً على مستخدمي أجهزة تكنولوجيا المعلومات والاتصالات. وتنبغي أيضاً حماية المستهلكين من الفصل التعسفي من الشبكات.
- وتعتمد مصادرة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة على التحقق المادي، وفي معظم الحالات، سيتخللها أو ستطلب عمل وكالات إنفاذ القانون التي تعتمد على إطار قانوني يدعم الإجراءات القضائية التي يمكن أن تنشأ. وتكمن التحديات في إقامة تعاون بين مختلف الوكالات، وتعريف إطار قانوني وتحديد المسؤولية عن أجهزة تكنولوجيا المعلومات والاتصالات المزيفة.
- وينبغي ألا يستهان بالتأثير على المستخدم. وينبغي أن يؤخذ في الاعتبار أن بعض البلدان قد لا تسمح بفصل أي جهاز وأن حياة المستخدم قد تتعرض للخطر جراء ذلك.

4.8 الحد من استيراد أجهزة تكنولوجيا المعلومات والاتصالات المزيفة الجديدة وتداولها وبيعها في السوق

ينبغي أن تنفذ التدابير التي تحد من استيراد أجهزة تكنولوجيا المعلومات والاتصالات المزيفة الجديدة وتهريبها وتداولها وبيعها في السوق بالإضافة إلى الإجراءات الرامية إلى سحب تلك الموجودة في المخزونات أو قيد الاستخدام.

ويمكن أن يساعد هذا النهج على خفض الوجود الكلي لأجهزة تكنولوجيا المعلومات والاتصالات المزيفة في السوق ضمن القيود المالية والزمنية للإدارة التي تختار اتخاذ هذه الإجراءات والحد من تأثيرها على المستخدم النهائي بالمقارنة مع الإجراءات التي تهدف إلى قطع الاتصالات وتكنولوجيا المعلومات المزيفة عن الشبكة.

وكما ورد في الفقرة 2.8، ينبغي أن تركز هذه التدابير أيضاً على مصادر أجهزة تكنولوجيا المعلومات والاتصالات المزيفة.

5.8 التفريق بين أجهزة تكنولوجيا المعلومات والاتصالات الأصلية والمزيفة

تقتضي الضرورة تنفيذ حلول ومعايير قادرة على التفريق بين الأجهزة الأصلية والمزيفة لضمان فعالية الإجراءات الرامية لسحب أجهزة تكنولوجيا المعلومات والاتصالات المزيفة المنتشرة في الأسواق وردع دخول الحديد منها. ويتعين أداء ذلك بدقة كبيرة حتى عند النظر في المعارف الفريدة المستنسخة، بحيث يمكن اتخاذ الإجراءات التعطيلية من خلال أنظمة مؤتمتة على نحو مفضل أو يدوياً لعدد محدود من أجهزة تكنولوجيا المعلومات والاتصالات.

وينبغي النظر في الجوانب التالية عند التفريق بين أجهزة تكنولوجيا المعلومات والاتصالات الأصلية والمزيفة:

- يتمثل هدف المزيف في إنتاج منتج قريب جداً من المنتج الأصلي الحقيقي.
- قد يلجأ المزيفون في سعيهم لتضليل التفتيش إلى تقديم وثائق وعتاد وبرمجيات أصلية مزورة أو مسروقة كجزء من التزييف الذي يقومون به.
- يمكن أن تأتي بعض عناصر المنتج المزيف من منتج أصلي وملحقاته، بما في ذلك على سبيل المثال لا الحصر: برمجيات، ومكونات فريدة، وعتاد الغلاف، ولوحة الدارة الإلكترونية المطبوعة (PCB) وشرائح إلكترونية.
- تخضع المنتجات الأصلية لتحديثات البرمجيات الثابتة بانتظام، وذلك لأسباب أمنية في المقام الأول. ويسري ذلك أيضاً على التطبيقات وعلى بعض الملحقات. وعلى هذا النحو، يمكن أن تمثل "بصمة" الجهاز المحددة لمنتج أصلي تحدياً.
- في كثير من الأحيان، لن تكفي المعاينة البصرية لتمييز جهاز أصلي، وقد يتطلب الأمر المزيد من الخبرات التقنية أو الدعم التقني أو الاختبارات المعملية.

6.8 الحد من التأثير على مصنعي أجهزة تكنولوجيا المعلومات والاتصالات المعتمدة

ينبغي للحلول المستخدمة لمكافحة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة أن تحد بأكبر قدر ممكن من التأثير على مصنعي أجهزة تكنولوجيا المعلومات والاتصالات المعتمدة وأن تركز على أجهزة تكنولوجيا المعلومات والاتصالات المزيفة، وعلى المنتجين والمتاجرين بهذه المنتجات.

ولذلك، ينبغي تجنب المخططات التي تضيف تكلفة إضافية على صناعة جهاز مشروع والتخلص منه من جانب جهة تصنيع أصلية، لأنها دون قصد تفيد أيضاً المزيف الذي يعتمد عادة على أسعار أرخص لاستمالة المستهلكين الذين يعتمدون اختيار جهاز تكنولوجيا المعلومات والاتصالات المزيف.

7.8 الحد من التأثير على المستخدم النهائي عند النظر في سحب أجهزة تكنولوجيا المعلومات والاتصالات المزيفة

ينبغي لأي حل يُعتمد لسحب أجهزة تكنولوجيا المعلومات والاتصالات المزيفة أو فصلها عن الشبكة أن ينظر بعناية في التأثير على المستخدمين النهائيين، وعندما تتاح مسارات متعددة لتحقيق الهدف نفسه، ينبغي أن يُعتمد الحل الذي يقلل من التأثير الإجمالي على المستهلك.

لذلك، ينبغي النظر في التحديات التالية:

- قد لا يُسمح بفصل أجهزة تكنولوجيا المعلومات والاتصالات في بعض البلدان.
- يتعذر الاتصال بالمستخدمين دائماً عبر الجهاز قبل فصله (ومثال ذلك أجهزة البيانات أو خدمة الرسائل النصية القصيرة فقط، وأجهزة إعادة تسيير مكالمات، وأنظمة الرد الصوتي التفاعلي (IVR)، وغيرها، التي يتعذر الاتصال عبرها بالمستخدم).
- قد يكون الحظر حرجاً على أجهزة تكنولوجيا المعلومات والاتصالات المزيفة التي تدعم الأعمال الحرجة (مثل التطبيقات الطبية والخدمات المالية وغيرها).
- ضمان عدم انتهاك حقوق المستخدم، واتخاذ مثل هذا الإجراء وفقاً للتشريعات الوطنية.

8.8 تثقيف المستهلكين

ينبغي تثقيف المستهلكين بشأن القضايا المرتبطة بشراء أجهزة تكنولوجيا المعلومات والاتصالات المزيفة واستخدامها، بما في ذلك على سبيل المثال لا الحصر، المخاطر الصحية المحتملة وسوء نوعية الخدمة.

ويجب الأخذ في الاعتبار أن المستهلكين كثيراً ما يتخذون قراراً متعمداً بشراء سلع مزيفة على أساس السعر، على الرغم من العواقب المحتملة، وبالتالي فإن زيادة وعي المستهلكين بالأثر السلبي لاستخدام تكنولوجيا المعلومات والاتصالات المزيفة ومزايا الأجهزة الأصلية أمر ضروري.

9.8 تجنب الحواجز التقنية المعوّقة للتجارة (TBT)

ينبغي الحرص على عدم منع استيراد أجهزة تكنولوجيا المعلومات والاتصالات الأصلية واستخدامها، الأمر الذي من شأنه أن يشكل "حاجزاً تقنياً معوقاً للتجارة (TBT)" على النحو المحدد في جوانب حقوق الملكية الفكرية المتصلة بالتجارة (WTO) لدى منظمة التجارة العالمية (TRIPS) [b-TRIPS Agreement].

وقد يشمل ذلك استخدام "القوائم البيضاء" التي يمكن أن تمنع، عن طريق الخطأ أو قرار التصميم السيئ، المستخدمين الشرعيين، بمن فيهم المسافرون والسياح، من استخدام أحد أجهزة تكنولوجيا المعلومات والاتصالات. ويمكن لمثل هذه المتطلبات الداعية لتسجيل الأجهزة أن تنشئ عن غير قصد حاجزاً تقنياً معوقاً للتجارة.

9 متطلبات الإطار

عند تنفيذ حل للتعامل مع أجهزة تكنولوجيا المعلومات والاتصالات المزيفة، ينبغي للبلدان أن تأخذ المتطلبات التالية بعين الاعتبار:

1.9 إجراءات التعرف والإنفاذ ضد منتجي ومهربي الأجهزة المزيفة

يلزم إنشاء عملية لاقتفاء أثر أجهزة تكنولوجيا المعلومات والاتصالات المزيفة وصولاً إلى مصدرها وإزالة المنتجين والمتاجرين الذين نشروا هذه المنتجات من السوق، وذلك بالتوازي مع مكافحة استخدام ما نُشر منها في السوق أو دخل إلى البلد.

وبما أن أجهزة تكنولوجيا المعلومات والاتصالات المزيفة كثيراً ما تمر عبر بلدان مختلفة قبل بيعها، تُتطلب إقامة تعاون قوي بين أصحاب المصلحة المعنيين بهذه العملية الجارية بين الأطراف النظيرة في البلدان المعنية الأخرى لاستيفاء هذا المطلب.

ويلزم اتخاذ إجراءات تعرف وإنفاذ ضد المنتجين والمتاجرين في اقتصادات المنشأ، على النحو الموضح في الفقرة 2.8.

2.9 التشاور مع دوائر الصناعة ومجموعات المستهلكين

تلزم إقامة اتصال مع جميع أصحاب المصلحة المعنيين، مثل مشغلي الشبكات ودوائر الصناعة ومجموعات المستهلكين، قبل اتخاذ أي إجراء تصحيحي، بحيث يمكن التشاور مع مبادرات دوائر الصناعة والتوصل إلى اتفاقات بشأن مسارات العمل المناسبة والمعقولة التي ستسفر عن الحد الأدنى من التعطيل للمستخدمين النهائيين.

وبالإضافة إلى ذلك، يمكن للمستهلكين أن يعوا التزاماتهم وحقوقهم فيما يتعلق باستخدام أجهزة تكنولوجيا المعلومات والاتصالات واقتنائها، ويمكن أن يقل التأثير السلبي لمكافحة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة على جميع أصحاب المصلحة. وينبغي بذل كل جهد لتقليل وتجنب أي خلل أو سوء فهم. وينبغي أن تكون جميع المعلومات المقدمة واضحة وسهلة الفهم للمستخدمين النهائيين.

ويلزم أيضاً تنفيذ إجراءات تركز على تعزيز تيسر الأجهزة وإمكانية النفاذ إليها وتثقيف المستهلكين، مما يوضح فوائد استخدام الأجهزة القانونية والآثار السلبية المرتبطة باستخدام المنتجات المزيفة.

3.9 المعرفات الفريدة الموثوقة

يُتطلب من أجهزة تكنولوجيا المعلومات والاتصالات الأصلية معرفات فريدة وثابتة وآمنة، بمعنى استعصاء تغييرها على يد جهات غير مجاز لها، وانفراد كل منها بجهاز من المعدات خصصت للمعرف له جهة تخصيص مجازة.

ويوصى المصنعون بتخزين هذا المعرف الفريد في عنصر آمن على المعدات وتنفيذ تدابير الأمن، إلى الحد الممكن عملياً، لكشف التلاعب بالمعرف الفريد، ونتيجة لذلك جعل الجهاز عصبياً على التشغيل إلى حين استرداد المعرف الأصلي.

وتوصى جهة إصدار المعرفات بتنفيذ عملية تضمن الاستخدام الصحيح والأمن لهذه المعرفات الفريدة.

4.9 قاعدة البيانات المرجعية المركزية

يوصى بنشر قاعدة بيانات مرجعية مركزية للمعدات المجازة في سوق محددة، بناءً على معرفات فريدة، للتمييز الفعال بين أجهزة تكنولوجيا المعلومات والاتصالات الأصلية والمزيفة.

وينبغي النظر في البنود التالية عند إنشاء قاعدة البيانات هذه:

- ينبغي تقاسم استعمال قاعدة البيانات المركزية هذه مع أصحاب المصلحة المعنيين في البلد، مثل السلطات الجمركية وشرطة الإنفاذ والهيئات التنظيمية، حتى تكون تلك المؤسسات على دراية بعبور البضائع، وعندئذ، تتمكن من وقف استيراد وتداول وبيع أجهزة تكنولوجيا المعلومات والاتصالات المزيفة الواردة إلى السوق ومن المساعدة في ملاحقة منتجي المنتجات المزيفة والمتاجرين بها.
- ينبغي أن تكون قاعدة البيانات المركزية هذه حجر الزاوية في الحل الذي يهدف إلى سحب الأجهزة المزيفة المستخدمة بالفعل في السوق.
- توجد قواعد بيانات سوق محددة يمكن أن تقدم معلومات عن المنتجات ضمن ذلك البلد، ويتألف بعضها من مجموعات فرعية طبيعية أو حتى مرتبطة بطريقة ما بقاعدة بيانات عالمية.

5.9 نشر نظام تقييم المطابقة

يلزم استخدام (أو إنشاء) مخطط تقييم المطابقة (CAS) القوي القائم لكفاءة نشر قاعدة بيانات مرجعية وطنية مركزية للمعدات المجازة، بناءً على شعارات اعتماد النوع أو الأيقونات أو غيرها من المعرفات الفريدة التي أنشأها مصنعو السلع الأصليين، بحيث يمكن لجميع أصحاب المصلحة (مثل سلطات الجمارك والعملاء ودوائر الصناعة) التفريق بين أجهزة تكنولوجيا المعلومات والاتصالات الأصلية والمزيفة.

- وضعت عدة إدارات وطنية، ومنظمات إقليمية ودولية، وشركات خاصة، والعديد من مشغلي تكنولوجيا المعلومات والاتصالات، مخطط تقييم مطابقة على أرض الواقع. وكعرف عام، عندما يتعلق الأمر باستخدام تكنولوجيا المعلومات والاتصالات على نطاق عالمي، تتبع الأجهزة الضرورية مجموعة من المعايير المقبولة دولياً وتمر عبر إجراءات تقييم المطابقة. (على سبيل المثال، الإقرار الصادر عن مختبر الاتحاد الدولي للاتصالات - CASC و ISO/CASCO و IECCEB و GSM و FCC و Innovation, Science and Economic Development Canada و ANATEL و GCF و PTCRB و ARIB وما إلى ذلك).

- تحتفظ هذه المنظمات بكمية كبيرة من البيانات المتعلقة بمراقبة المنتجات، ومنها على سبيل المثال: الجهات المسؤولة عن تصنيع هذه المنتجات وبيعها؛ ومجموعة المعايير واللوائح الوطنية (كتلك الخاصة بتوزيع الطيف) ومنشأ المنتجات.
- تتعدد طرق المضي قدماً في إنشاء سوق منظم لتكنولوجيا المعلومات والاتصالات. ومن الأمثلة على ذلك: في إطار الدعامة 4 في برنامج الاتحاد الدولي للاتصالات للمطابقة وقابلية التشغيل البيئي، وُضعت مبادئ توجيهية مختلفة. ويمكن العثور على البوابة الإلكترونية للمطابقة وقابلية التشغيل البيئي على الرابط: (<http://www.itu.int/en/ITU-T/C-I/Pages/default.aspx>).

6.9 التعاون الوثيق مع سلطات الجمارك والوكالات المحلية المناسبة

- للحد بشكل فعال من تداول أجهزة تكنولوجيا المعلومات والاتصالات المزيفة الجديدة واستيرادها وبيعها في السوق، تلزم إقامة تعاون وثيق بين السلطات المسؤولة عن قاعدة البيانات المرجعية الوطنية المركزية وسلطات الجمارك وبين الجمارك في البلدان المتميزة.
- بما أن السلطات الجمركية وغيرها من سلطات المستهلكين المحليين المجازين على الصعيد الوطني تؤدي دوراً حاسماً في اعتراض المنتجات المزيفة، فمن المهم تزويدها بالأدوات اللازمة للتعرف على أجهزة تكنولوجيا المعلومات والاتصالات المزيفة، مثل قاعدة البيانات المرجعية الوطنية المركزية.
- تمكن مكافحة الاتجار غير المشروع بأجهزة تكنولوجيا المعلومات والاتصالات، بما في ذلك الأجهزة المزيفة والمهزّبة والمسروقة، عن طريق استخدام آليات للاستيقان من هوية جهاز فردي للتحقق من أنه المادة الأصلية إذا سمحت بذلك القوانين واللوائح المعمول بها في ذلك البلد.
- ويجب وضع إجراءات الإنفاذ والاتصالات بين المنظمات المختلفة وتشغيلها بالكامل. ويمكن أن يشمل ذلك تبادل المعلومات ذات الصلة، مثل قاعدة البيانات الوطنية لأجهزة تكنولوجيا المعلومات والاتصالات بما يتماشى مع المعايير الوطنية أو الإقليمية أو الدولية.
- يوصى بأن تعتمد الجمارك منصة حكومية دولية على الإنترنت تتبادل معلومات المنتجات والتنبيهات التي تساعد في التعرف على المعدات المزيفة، مثل منظمة الجمارك العالمية (IPM) [b-WCO-IPM].

7.9 تبادل المعلومات مع المستخدم النهائي قبل أي إجراء تصحيحي

- يلزم إعلام المستهلكين بمخاطر شراء أجهزة تكنولوجيا المعلومات والاتصالات المزيفة وبأن مثل هذه الأجهزة قد لا تكون آمنة للاستخدام، وقد لا يجاري أداؤها أداء المواد الأصلية.
- وعلاوة على ذلك، يجب أن تُشرح للمستهلكين بوضوح دوافع عدم السماح بأجهزة تكنولوجيا المعلومات والاتصالات المزيفة من قبيل مخاطر المساس بالسلامة وانخفاض جودة الخدمة وبالتالي زيادة الشكاوى ومخاطر التداخل وانتهاك حقوق الملكية الفكرية (IPR)، وما إلى ذلك، وينبغي تنفيذ أي معلومات خاطئة لاحقة عن دواعي الإجراءات قد تتسبب في تأثيرات على السوق.
- وفي حال وضع حلول تكنولوجية للتعرف على أجهزة تكنولوجيا المعلومات والاتصالات المزيفة، يوصى بتقديم أداة لعامة الناس للتحقق من أصالة المنتج.

8.9 دعم الأطر القانونية والتنظيمية الوطنية السارية

- قبل تنفيذ أي إجراءات تقييدية ضد أجهزة تكنولوجيا المعلومات والاتصالات المزيفة، يلزم الحصول على دعم من الإطار القانوني والتنظيمي الوطني الساري، بما يشمل:
 - الحد من تفعيل أجهزة تكنولوجيا المعلومات والاتصالات المزيفة على شبكات الاتصالات؛
 - فرض قيود في السوق على استيراد وتداول وبيع أجهزة تكنولوجيا المعلومات والاتصالات المزيفة وملحقاتها التي لا تلتزم بالإطار التشريعي والتنظيمي في البلاد؛
 - وضع السلطات والمستهلكين وقنوات البيع للحلول اللازمة للتفريق بين المنتجات الأصلية والمزيفة؛

- تعزيز التدابير الأمنية بما يردع تصنيع المنتجات المزيفة والأخرى غير القانونية؛
 - وضع إطار قانوني ضد العبث بالمعرفات الفريدة.
- وعند النظر في هذه المتطلبات، ينبغي الاحتكام إلى التشريعات الوطنية والأطر التنظيمية القائمة التي قد تعالج أصلاً الجوانب المشمولة.

9.9 مراعاة المنتجات المستخدمة الآن في السوق

قبل اتخاذ أي إجراء تعطللي لأجهزة تكنولوجيا المعلومات والاتصالات المزيفة في السوق، يوصى بالنظر في ضرورة حماية مستخدمي هذه المنتجات. ومن شأن ذلك أن يخفف من التأثير السلبي على مستخدمي هذه الأجهزة الذين يجهلون الأحكام أو المتطلبات القانونية أو التنظيمية الوطنية المتعلقة بشراء واستخدام أجهزة تكنولوجيا المعلومات والاتصالات المزيفة هذه.

وقد يؤدي حجب أجهزة تكنولوجيا المعلومات والاتصالات الجاهزة للتشغيل إلى آثار ثقيلة وغير متوقعة على أنواع مختلفة من الشبكات والمستخدمين النهائيين والبنية التحتية. وفي هذه الحالة، يتمثل أحد الخيارات في اعتماد آليات انتقالية قابلة للتطبيق، مثل البدء بحجب المطاريف الجديدة فقط، والسماح للأجهزة الموجودة بالفعل على الشبكة بمواصلة العمل، ولكن سيتعين على المستخدمين، في نهاية المطاف، الانتقال إلى مطاريف أصلية.

10 نهج حل ممكنة لتكنولوجيا المعلومات والاتصالات المزيفة

بالنظر إلى المتطلبات المذكورة أعلاه واستناداً إلى المعلومات المقدمة في دراسات الحالة الواردة في التقرير التقني لقطاع تقييس الاتصالات [b-ITU-T TR-Counterfeit] والمستقاة من مصادر أخرى، فإن ما يلي يمثل بعض الأساليب الممكنة لمكافحة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة وبعض الاعتبارات التي ينبغي احتسابها عند نشر بعض من هذه الحلول:

1.10 حظر استخدام معرفات جهاز غير صحيحة وغير أصلية

إذا استخدم الجهاز معرفاً فريداً للتسجيل على الشبكة، فيمكن رفض هذا التسجيل للأجهزة المزيفة من خلال استخدام قاعدة بيانات الأجهزة المجاز تشغيلها في أسواق معينة.

وفي هذه الحالات، إذا كان جهاز تكنولوجيا المعلومات والاتصالات يمتلك معرفاً فريداً موثقاً، يمكن نشر حلول من شأنها:

- حظر المعدات ذات المعرفات الفريدة غير الصالحة على شبكاتهم؛
- ومنع استخدام المعدات التي لا يعتمدها المنظم؛
- ومنع الاستيراد غير القانوني والبيع لهذه الأجهزة.

وإذا اختير مسار الإجراءات هذا، يوصى أيضاً بتوعية المستهلك بهذه المتطلبات. وبالإضافة إلى ذلك، قد يلزم اعتماد تغييرات تشريعية مناسبة على المستوى الوطني على النحو الموضح في الفقرة 8.9 أعلاه.

وعند اعتماد حل لمكافحة أجهزة تكنولوجيا المعلومات والاتصالات المزيفة من خلال تحديد وحظر الأجهزة ذات شفرات المعرف الفريد غير الصالحة، قد يساعد هذا الحل أيضاً فيما يلي:

- ضمان عدم استيراد أو بيع إلا الأجهزة القانونية مما يؤثر على زيادة مدفوعات الرسوم الجمركية وضريبة القيمة المضافة؛
- ومكافحة سرقة الأجهزة بتسجيل شفرات المعرفات الفريدة للمعدات المسروقة في "القائمة السوداء" بناء على طلب قانوني؛
- وضمان حماية المستهلك من استخدام معدات منخفضة الجودة التي قد تكون غير مجازة أو خطيرة على صحة الإنسان أو التي لا تضمن جودة كافية للخدمات (تضمن الحماية بتنفيذ أداة لتسهيل التحقق من قانونية المعدات قبل شرائها).

وينبغي توخي الحذر في عملية المعايير لاحترام حماية المعلومات الشخصية وعدم التأثير سلباً على مستخدمي أجهزة تكنولوجيا المعلومات والاتصالات من خلال آليات تسجيل المعرف. وتنبغي أيضاً حماية المستهلكين من الفصل التعسفي من الشبكات.

ويمكن الاطلاع على مزيد من المعلومات عن إمكانية تنفيذ حل أُعد للأجهزة المتنقلة في الملحق A.

2.10 إصدار شهادات لأجهزة تكنولوجيا المعلومات والاتصالات ومراقبة السوق

كما أشير في الفقرة 5.9، يمكن لنشر مخطط تقييم المطابقة (CAS) أن يساعد في بناء قاعدة بيانات مرجعية وطنية للمعدات المجازة التي تحتوي على قائمة بالمعرفات الفريدة ومعلومات إضافية للأجهزة (مثل علامات الموافقة، والمواصفات التقنية، والخصائص المادية)، بحيث يمكن لجميع أصحاب المصلحة (مثل السلطات الجمركية والعملاء ودوائر الصناعة) التعرف على الأجهزة المعتمدة.

ويمكن لمسؤولي الجمارك كذلك بهذه المعلومات التعرف على المنتجات المزيّفة بفرض مراقبة السوق وتدابير إنفاذ أخرى قد تدعو إليها الحاجة. وبالإضافة إلى ذلك، يمكن تحديد المستوردين ذوي السوابق في تجاهل ضوابط الاستيراد ووضعهم على قائمة خاصة. وعندما يستورد المهريون شحنات أجهزة تكنولوجيا المعلومات والاتصالات، يمكن إخطار السلطات التنظيمية بحيث يتسنى اتخاذ قرار للقيام بعمليات تفتيش، وينبغي بعد ذلك أن يكون الإنفاذ مسوَّغاً.

وكجزء من سياسة مخطط تقييم المطابقة، تهدف مراقبة السوق لمعدات الاتصالات المنفّذة إلى ضمان عدم تسبب المنتجات الموضوعة في السوق في حدوث تداخل كهرومغناطيسي، أو الإضرار بشبكة الاتصالات العامة، أو تهديد الصحة أو السلامة أو أي جانب آخر من جوانب حماية عامة الناس.

وفي الممارسة العملية، تشمل مراقبة السوق أي من الإجراءات الضرورية (مثل الحظر والسحب والاستعادة) لوقف تداول المنتجات التي لا تتمثل لجميع المتطلبات المنصوص عليها في التشريعات واللوائح ذات الصلة وفرض المطابقة على المنتجات وتطبيق العقوبات. ومراقبة السوق أمر حيوي لسلاسة أداء سوق الاتصالات. وهي أساسية لحماية المستهلكين والعمال من المخاطر التي تنطوي عليها المنتجات غير المتزامنة. وبالإضافة إلى ذلك، تساعد مراقبة السوق على حماية مصالح الأعمال المسؤولة ضد المنافسة غير العادلة من جهات تشغيل اقتصادي مستهترّة تتجاهل القواعد أو تتنصل من تكاليفها.

وللعديد من الهيئات التنظيمية في جميع أنحاء العالم متطلبات قانونية محددة لتنظيم مراقبة السوق. وتحدد اللوائح عادةً التزامات واضحة لسلطات مراقبة السوق، تنص على أن تكون لديها السلطات والموارد والمعرفة اللازمة لأداء وظائفها على الوجه الصحيح [b-ITU-T-CI-Portal]. وتتطلب اللائحة وضع إجراءات المتابعة الشكاوى ومراقبة الحوادث والتحقق من اتخاذ إجراءات تصحيحية وجمع المعارف العلمية والتقنية المتعلقة بمسائل السلامة. وإضافة إلى ذلك، تقوم الدول الأعضاء في الاتحاد بوضع وتنفيذ برامج مراقبة السوق الوطنية وتحديثها دورياً واستعراض وتقييم أداء أنشطة المراقبة الخاصة بها دورياً، كل بضع سنوات على سبيل المثال. [b-ITU-D-CI-Guidelines]

وتعرّف لائحة المفوضية الأوروبية رقم 765/2008 مراقبة السوق على أنها: الأنشطة التي نفذتها السلطات المعيّنة والتدابير التي اتخذتها لضمان توافق المنتجات مع المتطلبات المنصوص عليها في التشريعات ذات الصلة، وعدم تهديدها للصحة أو للسلامة أو لأي جانب آخر من جوانب حماية المصلحة العامة. [b-EC-Regulation]

ولذلك، لاستكمال الإجراءات التي تُتخذ في اللحظة التي يصل فيها المنتج إلى حدود البلاد، يوصى بإجراء مراقبة إضافية بعد التسويق للمساعدة في التعرف على السلع المزيّفة وبالتالي ضمان توافق المنتج الذي يباع للمستخدم النهائي في الواقع مع الذي قُدم لاستصدار شهادة له. [b-ITU-D-Rep]

وتوصي لجنة الأمم المتحدة الاقتصادية لأوروبا (UNECE) بتنسيق مراقبة السوق الوطنية مع أنشطة جمارك وبتمكن أصحاب الحقوق من إبلاغ سلطات مراقبة السوق عن المنتجات المزيّفة [b-UNECE].

3.10 إدارة دورة حياة الجهاز

تُستحسن القدرة على التمييز بين جهاز تكنولوجيا المعلومات والاتصالات الأصلي وآخر مستنسخ، دون المساس بحقوق المستخدم. وعادة ما تسيء هذه الأجهزة المستنسخة استخدام المعرفات أو عناصر تعريف فريد أخرى، لتزعم أنها أجهزة أصلية.

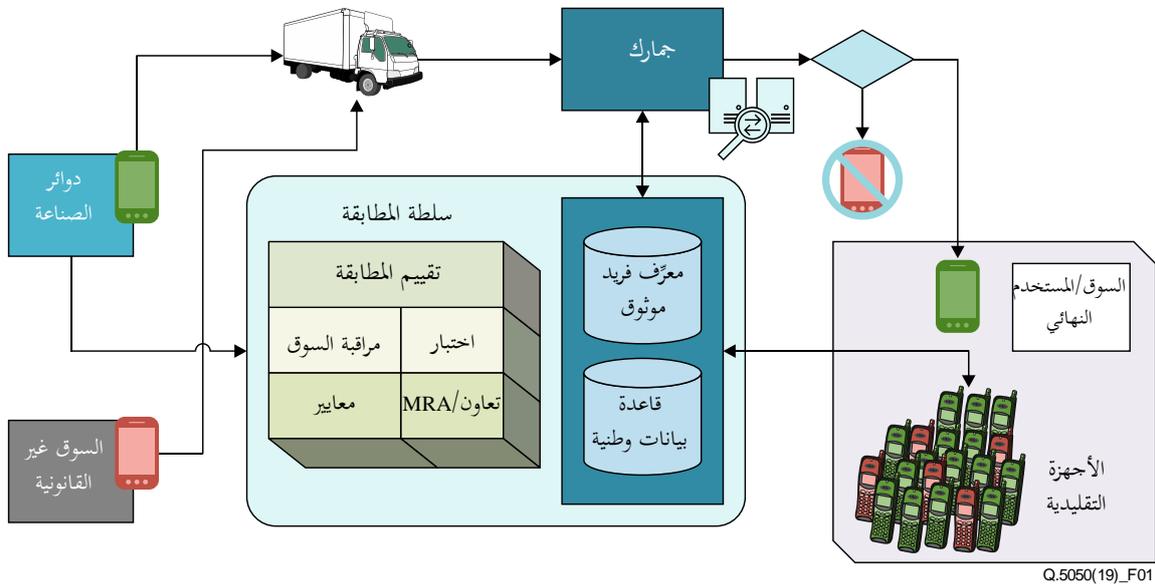
وأحد الحلول الممكنة، لمساعدة أصحاب المصلحة هؤلاء وضمان أصالة أجهزة تكنولوجيا المعلومات والاتصالات، ينبغي أن يتمثل في نشر نظام إدارة دورة حياة الجهاز، استناداً إلى هذه المعرفات الفريدة، القادرة على تتبع أجهزة تكنولوجيا المعلومات والاتصالات بدءاً من عملية تصنيعها (بما في ذلك منشأ المكونات، ونقلها وإيداعها في متاجر التجزئة ليصار إلى بيعها) حتى تسليمها إلى المستخدم النهائي.

وينبغي أن تتاح هذه المعلومات لجميع أصحاب المصلحة، وعندئذ رغم أن التزيف يمكن أن يستنسخ المعارف الفريدة، ستمتكن السلطات وحتى المستخدم النهائي من التحقق من صحة هذه المعلومات. وعلى سبيل المثال، إذا كان أحد المستخدمين في متجر في بلد ما، وبالتحقق من المعرف الفريد، بينت الأداة أن المنتج يُفترض ببيعه لدى بائع تجزئة آخر أو حتى في بلد آخر، ينبغي أن يكون ذلك دليلاً قوياً على أن المنتج مزيف حتى بوجود معرف فريد صالح.

وينبغي توخي الحرص عند استخدام هذا النوع من الحلول أثناء معالجة قيام المستخدم النهائي بإعادة بيع المنتجات المستخدمة، حيث ينبغي أن تراعي التشريعات الوطنية التأثير على حماية المعلومات الشخصية عند الربط بين المستخدم والجهاز الحارية إدارته. وينبغي أن يعتبر أن المنتج الذي يُعرف عليه من خلال هذا النوع من النُهُج قد لا يكون مزيفاً، بل منتجاً أصلياً يباع في سوق موازية، وستدعو الحاجة إلى إجراءات إضافية للتعرف على منتج مزيف.

11 الإطار المرجعي

استناداً إلى النقاط المشتركة للنُهُج المختلفة الممكنة المعروضة في الفقرة 10، يرد في الشكل 1 إطار مقترح لمعالجة إنتاج أجهزة تكنولوجيا المعلومات والاتصالات المزيفة وتداولها واستخدامها:



الشكل 1 - الإطار العام المقترح

ينبغي أن تعمل معاً مجموعة متنوعة من الأنشطة وأنظمة المعلومات، التي تشغلها منظمات مختلفة، للتحكم في المعلومات الهامة وإنتاجها للتعرف على الأجهزة المزيفة والمتلاعب بها ومكافحة استخدامها.

وتسمح التجارة القانونية بالتحقق من أن المنتج الذي يدخل البلد ملتزم وله ممثل/مسؤول عن المعدات.

وعندما تصل المنتجات إلى نقطة تحكم، تتحقق جهة (الجمارك، على سبيل المثال) من جميع الجوانب القانونية لهذه الأجهزة، بما في ذلك التزام الأجهزة بأي متطلبات تنظيم وإشهاد سارية مثل توزيع الترددات الراديوية والسلامة وقابلية التشغيل البيني وما إلى ذلك. ويمكن أيضاً مراجعة القائمة البيضاء للأجهزة¹ للتحقق من أن معارف الأجهزة الجاري استيرادها قد وُزعت بشكل مشروع وأن طراز ونموذج الجهاز الجاري فحصه يتوافقان مع التفاصيل المسجلة عند إصدار المعارف.

¹ على سبيل المثال، يمكن استخدام قاعدة بيانات GSMA Global TAC للمساعدة في إنشاء قائمة بيضاء للأجهزة الملتزمة بمتطلبات 3GPP.

وفي الوقت الحالي، تُمنع المنتجات غير المجازة، كالمنتجات المزيفة، من دخول السوق. ويُدعم موظفو الجهة المعنية بنظام تقييم مطابقة قد يكون موجوداً وقاعدة بيانات تحتوي على معلومات مخزنة عما ينبغي أن يكون في الحاويات الجاري استيرادها. ويمكن لقواعد بيانات الجرد هذه أن تدعم أنشطة الإنفاذ بمجرد وضع المعدات (القانونية أو غير القانونية) في السوق.

الملحق A

حلول الأجهزة المتنقلة

(يشكل هذا الملحق جزءاً أساسياً من هذه التوصية)

عند التعامل مع الأجهزة المتنقلة المتوافقة مع متطلبات 3GPP، تستند بعض حلول التعرف على المطايف المتنقلة الأصلية والمستوردة قانونياً إلى استخدام نظام تسجيل الهوية الدولية للمعدات المتنقلة (IMEI). وتستند الحلول التي تعتمد على الهوية الدولية للمعدات المتنقلة لردع انتشار الهواتف المتنقلة المزيفة إلى التالي:

- حجب الأجهزة المتنقلة التي تحتوي على أرقام غير صالحة للهوية الدولية للمعدات المتنقلة (من قبيل عدم وجود رقم IMEI، أو رقم IMEI كله أصفار، أو سلاسل نسق غير معياري، أو أرقام IMEI مكررة، أو أرقام IMEI وزعتها منظمات غير مجازة، أو رقم IMEI صالح لم توزعه المنظمة المعنية بعد) عن الشبكات²،
- اتخاذ إجراءات أخرى بشأن توعية المستهلك وتدابير الإنفاذ وتغييرات مناسبة للتشريعات على المستوى الوطني.

ولمنع استخدام الأجهزة المتنقلة المزيفة، يمكن نشر النظام على أساس تسجيل كل شفرة هوية دولية صحيحة للمعدات المتنقلة (وهي معرّف وفقاً للمعايير مستورد قانونياً ومعتمد أو مجاز نوعاً، وتوزعه رسمياً مؤسسة معينة) تبين النشاط على الشبكات الوطنية. ويضمن تسجيل الهويات الدولية للمعدات المتنقلة التزام الأجهزة المتنقلة باللوائح الوطنية، ويضمن في بعض البلدان، استيرادها بشكل قانوني.

• قواعد البيانات المرجعية

تستخدم شفرات الهوية الدولية للمعدات المتنقلة لإنشاء قاعدة بيانات تحتوي على "القائمة البيضاء" و"القائمة الموازية" و"القائمة السوداء" للأجهزة. و"القائمة البيضاء" هي سجل للأجهزة المجاز استخدامها في البلد (مثل تلك التي جرى استيرادها أو تصنيعها بشكل قانوني في هذا البلد)، أما "القائمة الموازية" فهي سجل للأجهزة ذات الحالة (غير المؤكدة غير المدرجة في "القائمة البيضاء" أو "القائمة السوداء") و"القائمة السوداء" هي سجل للأجهزة التي يجب حرمانها من الخدمات في شبكة الاتصالات. وينبغي إجراء تحليل مسبق لماهية تأثيرات نشر "القائمة البيضاء" و"القوائم الموازية" و"القائمة السوداء" على الشبكات والمستخدمين، لأنها يمكن أن تحد من حركة الأجهزة بين البلدان، وأن تطل بتأثيرها الزوار الأجانب ومشغلي الشبكات. وتتولد "القائمة الموازية" و"القائمة السوداء" تلقائياً عن طريق معالجة البيانات المستقاة من "القائمة البيضاء" والبيانات المستقاة من المشغلين والمستوردين والسلطة الجمركية.

• التكامل مع شبكة المشغل

لضمان التفاعل النشط مع نظام التسجيل، يتعين على مشغلي الاتصالات الاحتفاظ بسجلات هوية المعدات (EIR) الخاصة بهم وضمان التزام المنتظم والتبادل التلقائي للبيانات بين سجلات المعلومات المرجعية وقاعدة بيانات شفرات الهوية الدولية للمعدات المتنقلة (يوميًا).

وعند أول توصيل وتسجيل لهاتف متنقل لدى أي مشغل شبكة، يُرسل مشغل الاتصالات المتنقلة تلقائياً شفرة IMEI العائدة للمطرف إلى قاعدة البيانات. ويكشف النظام شفرات الهوية الدولية للمعدات المتنقلة (IMEI) غير الواردة في القائمة "البيضاء"، ويحدد الهواتف المتنقلة المزيفة ويسجل ما يقابلها من شفرات الهوية الدولية للمعدات المتنقلة في القائمة "الموازية". ويتلقى مالك

² يمكن استخدام قاعدة بيانات GSMA Global TAC للتحقق من صحة الهويات الدولية للمعدات المتنقلة المختلطة أو المستنسخة للأجهزة المتوافقة مع متطلبات 3GPP.

المطراف المعني إشعاراً عبر خدمة الرسائل القصيرة (SMS) بهذا الشأن، ويتعين عليه تأكيد المصدر القانوني للمطراف في غضون مهلة محددة من تاريخ إدراجه في القائمة "الموازية".

وينبغي ضمان موثوقية وأمن نظام التسجيل والعمليات المرتبطة به. ويتاح النفاذ عموماً إلى هذه القوائم لسلطات التنظيم والجمارك ومشغلي الشبكات وعامة الناس بمستويات مناسبة من امتيازات النفاذ. وينبغي أن تتاح للمستخدمين إمكانية النفاذ إلى قاعدة البيانات هذه للتحقق مما إذا كان يُسمح بتشغيل جهاز متنقل في البلد (عادةً عن طريق إرسال رسالة عبر خدمة الرسائل القصيرة (SMS) أو استخدام صفحة ويب).

ويجدر بالذكر أن خدمة الرسائل القصيرة ينبغي اعتبارها وسيلة غير آمنة للتواصل مع أحد العملاء ويمكن للمحتالين استغلالها، لذلك قد تدعو الحاجة إلى إجراءات إضافية.

• كشف الهوية الدولية المستنسخة للمعدات المتنقلة

نظراً لإمكانية العبث بالمعرفات الفريدة لبعض الأجهزة، واحتمال أن يبدأ المتاجرون باستنساخ الهويات الدولية للمعدات المتنقلة العادية لتجنب هذا النظام، ينبغي تنفيذ إجراءات إضافية من أجل التعرف على الأجهزة غير النظامية ذات الهويات الدولية المستنسخة للمعدات المتنقلة المشروعة، والتصرف ضدها.

ويتمثل أحد المسارات الممكنة في اعتماد قواعد بيانات تحتوي على معلومات إضافية عن المنتج، يمكن استخدامها للتحقق مما إذا كان المنتج الذي يستخدم المعرفات مطابقتاً للسمات الأخرى. ويمكن تنفيذ هذه الأدوات بمساعدة دعم نظام تقييم المطابقة الذي من شأنه أن يجمع هذه المعلومات أثناء عملية إصدار الشهادة للجهاز وأن يخزنها في قاعدة بيانات يمكن لجميع أصحاب المصلحة النفاذ إليها.

• اعتبارات إضافية

إلى جانب ذلك، فإن حلاً لمكافحة الأجهزة المتنقلة المزيفة بتحديد وحجب الأجهزة المتنقلة ذات شفرات الهوية الدولية للمعدات المتنقلة غير الصالحة أو المتلاعب بها، قد يساعد فيما يلي أيضاً:

- منع الاستيراد غير القانوني لهذه الأجهزة، وبالتالي ضمان استيراد الأجهزة المتنقلة وبيعها بطريقة قانونية، ومن ثم زيادة مدفوعات الرسوم الجمركية وضريبة القيمة المضافة؛
- مكافحة سرقة الجهاز اليدوي عن طريق تسجيل شفرات الهوية الدولية للمعدات المتنقلة المسروقة في "القائمة السوداء" بناء على طلب قانوني، مما يجعل سرقة المطايرف عديمة الفائدة (يمكن تطبيق الإجراء نفسه على قفل المطراف بناء على طلب أصحاب أجهزة متنقلة مفقودة)؛
- منع استخدام معدات نوعها غير معتمد لدى الهيئة التنظيمية، وضمان حماية المستهلك من استخدام مطايرف متنقلة منخفضة الجودة، قد تكون غير مجازة أو خطيرة على صحة الإنسان أو قد لا تضمن جودة كافية للخدمات الاتصالات المتنقلة (وتُضمن الحماية بتنفيذ الأداة لتسهيل التحقق من قانونية الهاتف المتنقل قبل شرائه).

ومن المهم الحفاظ على نهج منسق على الصعيد الوطني، نظراً لإمكانية وجود أجهزة تكنولوجيا المعلومات والاتصالات المزيفة والأجهزة في أكثر من شبكة واحدة، وينبغي أن تتوخى عملية الكشف كفاءة الإجراءات التي يراد اتخاذها لتجنب التأثيرات على مستخدمين متعددين أو ازدواجية الجهود أو النزاعات عبر مختلف مشغلي الهواتف المتنقلة.

وينبغي القيام بتخطيط المراحل المبكرة من التشخيص (تحديد حجم مشكلة معرفات الهوية غير الصالحة والمستنسخة، وما إلى ذلك) في عملية الكشف والتحكم، والموارد المطلوبة (المال، والموظفين، والوقت)، وتحليل التأثيرات لتخفيف وطأتها على المستخدمين النهائيين، ومناقشة ذلك مع أصحاب المصلحة جميعهم لتنفيذ مثل هذه الحلول.

وينبغي أيضاً النظر في بعض الحالات حيث يمكن أن تتسبب هذه الآليات في مشاكل للمستخدمين الشرعيين، بمن فيهم المسافرون والسياح، ومثال ذلك:

- يمكن لمستخدم أجنبي، حين يسافر إلى بلد ما ثم يستخدم بطاقة وحدة تعريف هوية المشترك (SIM) المحلية في جهازه، أن يقع في فخ القائمة البيضاء حيث يعجز عن استخدام جهازه.
 - يمكن أيضاً للإدراج في قائمة بيضاء محلية أن يفرض عقوبة محففة على زائر اتصالات تجوال يستمر في استخدام جهازه لبضعة أشهر بعد فترة استخدام.
 - قد تُرسل رسالة تسجيل إلى أحد الزوار لبلد يستخدم شريحة SIM محلية، إلا أنه قد لا يتحدث اللغة المحلية ولا يمكنه فهم الرسالة. وبالتالي لا يبادر إلى التسجيل ويُدرج جهازه على القائمة السوداء. وهذا إما: '1' بسبب فصل الزائر عن الشبكة المحلية؛ أو '2' يتسبب في إدراج الجهاز المشروح للزائر في القائمة السوداء في البلدان الأخرى جراء ترتيبات تبادل المعلومات، على الرغم من كون الجهاز مشروعاً تماماً.
- وعلى هذا النحو، يمكن أن تؤدي هذه الآليات، في حال سوء التنفيذ، إلى وقوع مشاكل وينبغي تجنب هذه السيناريوهات من خلال التصميم. وأخيراً، يجب عدم استخدام هذه الخواص الوظيفية لفصل المستخدمين عن الشبكات بشكل تعسفي لأسباب أخرى.

التذييل I

الحلول الأخرى لدى دوائر الصناعة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

استثمرت دوائر الصناعة في جهود متعددة للتصدي لمشكلة المعدات المزيفة ولتحسين موثوقية المعدات والشركات. وتلك هي الجهود التي تقودها دوائر الصناعة لتطوير حلول طوعية لتعزيز أمن سلسلة التوريد. وتعد المعدات المزيفة أحد جوانب هذه الجهود، ولكنه ليس وحيداً. إذ يجب أن تعمل دوائر الصناعة أيضاً مع الحكومات، وعلى وجه التحديد مع سلطات إنفاذ القانون والجمارك من أجل الإنفاذ. ومن الأفضل التفكير في نتائج هذه الجهود كأداة يمكن للشركات اللجوء إليها حسب الحاجة والظروف المحددة (على سبيل المثال، المنتج، السوق، وما إلى ذلك).

ويلاحظ أن الأنشطة الصناعية بشأن المنتجات المزيفة تغطي مجموعة واسعة جداً من المنتجات ذات سلاسل التوريد المتنوعة، ولبعضها احتياجات مختلفة. وهذا تفاعل معقد مع جهات مشاركة متعددة. وبالإضافة إلى هذه الأنشطة الخارجية، تنفذ الشركات أعمال بحث وتطوير عالية الحساسية والسرية لإعداد طرق لمكافحة التزييف.

وترد أدناه نظرة عامة غير شاملة على بعض الجهود الرامية لتعزيز أمن الجهاز يمكنها أن تساهم في جعل التزييف أكثر صعوبة.

• قاعدة بيانات الهوية الدولية للمعدات المتنقلة لدى رابطة النظام العالمي للاتصالات المتنقلة (GSMA)

الهوية الدولية للمعدات المتنقلة هي رقم مكون من 15 خانة رقمية يُستخدم للتعرف على جهاز على شبكة الاتصالات المتنقلة. وشفرة توزيع النوع - TAC هي أولى 8 خانات رقمية من الهوية الدولية للمعدات المتنقلة وهي تحدد نموذجاً محدداً.

وتدير رابطة النظام العالمي للاتصالات المتنقلة (GSMA) قاعدة بيانات عالمية تحتوي على معلومات عن شفرات توزيع النوع المحددة - TAC التي تُخصص للأجهزة الملتزمة بمتطلبات 3GPP. وتُعرف قواعد البيانات هذه باسم قاعدة بيانات الهوية الدولية للمعدات المتنقلة.

ويمكن استخدام قاعدة البيانات هذه بالطرق التالية:

- يمكن تحديد هوية أجهزة تكنولوجيا المعلومات والاتصالات المزيفة بالتعاون مع المصنِّع الأصلي الذي يمكن تحديده باستخدام قائمة قاعدة بيانات TAC GSMA.
- تمكن إتاحة قاعدة بيانات TAC GSMA لجهات حكومية، مثل الوزارات والهيئات التنظيمية والجمارك وسلطات إنفاذ القانون، كمصدر للمعلومات عن مصدر الأجهزة المتنقلة ومواصفاتها. ويمكن استخدام هذه المعلومات للوقوف على الحالات الشاذة وتحديد منتج الجهاز الذي لا يمكنه تأكيد ما إذا كان الجهاز أصلياً أم لا.
- يمكن التحقق من صحة منتجي الأجهزة المتنقلة والهوية الدولية للمعدات المتنقلة الخاصة بهم باستخدام قاعدة بيانات TAC GSMA. ويمكن لوكالات الجمارك وإنفاذ القانون استخدام مكتب المساعدة لدى رابطة النظام العالمي للاتصالات المتنقلة (GSMA) للتحقق من الرقم التسلسلي لشهادة TAC المقدمة من المنتج. وهذا هو الرقم التسلسلي الثاني المرتبط بكل شفرة TAC. ويشي عدم التطابق بين هذه المعرفات إلى شكل ما من تزوير المعرف.
- يمكن للهيئات التنظيمية استخدام قاعدة بيانات TAC GSMA لضمان مطابقة الأجهزة المتنقلة الجاري اختبارها في تقييم التوافق لوصف النموذج المدرج في قاعدة البيانات.

قاعدة بيانات الهوية الدولية للمعدات المتنقلة لدى رابطة النظام العالمي للاتصالات المتنقلة (GSMA):

<https://imeidb.gsma.com/imei/index>

خدمات الهوية الدولية للمعدات المتنقلة لدى رابطة النظام العالمي للاتصالات المتنقلة (GSMA):

<https://www.gsma.com/services/tac-allocation/the-imei-database/>

• نظام التعرف على الجهاز وتسجيله وحجبه (DIRBS)

نظام التعرف على الجهاز وتسجيله وحجبه (DIRBS) هو منصة برمجيات قائمة على مخدم تهدف إلى التعامل مع الأجهزة المتنقلة المزيفة وغير القانونية والمسروقة في بلد ما. وتتوفر منصة برمجيات DIRBS كمصدر مفتوح لمساعدة الحكومات والهيئات التنظيمية وغيرها في جهودها لمكافحة الاستخدام غير المشروع للأجهزة المزيفة وغير القانونية والمسروقة على الشبكات الخلوية. وتتسق المنصة مع توصيات الاتحاد الدولي للاتصالات في التعامل مع الأجهزة غير القانونية وغير معتمدة النوع في أي بلد.

ويتألف نظام DIRBS من قاعدة بيانات الأجهزة على المستوى القطري ترتبط بمستويات مختلفة من التفاصيل مع المشغلين، والمصنعين المحليين، والمستوردين، والمستهلكين، والجمارك، وسلطات إنفاذ القانون، وقاعدة بيانات الهوية الدولية للمعدات المتنقلة لدى رابطة النظام العالمي للاتصالات المتنقلة. ويتألف نظام DIRBS من محرك التحليل والأنظمة الفرعية المرتبطة به التي تقدم المعلومات اللازمة لتمكين حظر الأجهزة المزيفة والمزورة؛ ويتحدد الحجب الفعلي وفقاً للقواعد الناظمة الخاصة بكل بلد ويجرى من خلال آليات تسجيل هوية المعدات (EIR) لدى المشغل.

ويمكن الاطلاع على معلومات أوفى عبر الرابط التالي: www.qualcomm.com/dirbs

• مجموعة الحوسبة الموثوقة

"مجموعة الحوسبة الموثوقة (TCG) هي منظمة غير هادفة للربح شُكلت لوضع وتعريف وترويج معايير الصناعة العالمية المحايدة تجاه منافذ البيع، والداعمة لجذر الثقة القائم على العتاد، من أجل منصات حوسبة موثوقة قابلة للتشغيل البيئي".

ومن بين مجالات أخرى، قامت مجموعة TCG بوضع مواصفات لوحات المنصة الموثوقة ذات الصلة بهذا الموضوع:

http://www.trustedcomputinggroup.org/resources/tpm_main_specification

http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary

وكما جاء في الموقع الإلكتروني المذكور أعلاه، فإن وحدة المنصة الموثوقة (TPM) هي رقاقة حاسوب (وحدة تحكم صغيرة) يمكنها أن تخزن على نحو آمن مصنوعات تُستخدم للاستيقان من المنصة (حاسوب أو حاسوب محمول). ويمكن أن تشمل هذه المصنوعات كلمات مرور أو شهادات أو مفاتيح تجفير.

وتسمح هذه الآلية بإشهاد محلي وبعيد معاً يساعد على إرساء الثقة في أن المعدات أصلية.

واستحدثت مجموعة TCG أيضاً فريق عمل للأنظمة المدججة لمعالجة أمن الأنظمة المدججة، بما في ذلك إنترنت الأشياء (IoT):

http://www.trustedcomputinggroup.org/developers/embedded_systems

• المنصة العالمية (Global Platform)

قامت المنصة العالمية Global Platform بوضع معايير بيئة التنفيذ الموثوقة (TEE) التي اعتمدت في الأجهزة المتنقلة الحديثة كأسلوب آمن لتخزين وتنفيذ شفرة أمن وأصول حساسة.

ويمكن الاطلاع على معلومات أوفى عبر الرابط التالي: <https://www.globalplatform.org/specificationsdevice.asp>

• **اللجنة الخاصة 27 التابعة للجنة التقنية رقم 1 المشتركة بين المنظمة الدولية للتوحيد القياسي واللجنة الكهروتقنية الدولية (ISO/IEC JTC1 SC27)**

يُعتبر نطاق عمل اللجنة الخاصة 27 مهماً لأنشطة الصناعة المتعلقة بالأمن والتخفيف من التزييف ووضع معايير حماية المعلومات وتكنولوجيا المعلومات والاتصالات. وهذا يشمل الأساليب والتقنيات والمبادئ التوجيهية العامة لمعالجة الأمن وحماية المعلومات الشخصية على السواء.

ومن بين أعمالها الأخرى، نشرت اللجنة الخاصة 27 معايير ذات صلة بالمعدات المزيفة، مثل:

- [b-ISO/IEC 15408]: *Information technology – Security techniques – Evaluation criteria for IT security" (Common Criteria)*;
- [b-ISO/IEC 27034] *Information Technology – Security Techniques – Application Security*;
- [b-ISO/IEC 27036-3]: *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*;
- [b-ISO/IEC 20243]: *Information Technology – Open Trusted Technology Provider TM Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products.*

ويمكن الاطلاع على معلومات أوفى عبر الرابط التالي: <http://www.din.de/en/meta/jtc1sc27>

• **منتدى التكنولوجيا الموثوقة لدى المجموعة المفتوحة**

يقود منتدى التكنولوجيا الموثوقة لدى المجموعة المفتوحة (OTTF) تطوير برنامج وإطار سلامة سلسلة التوريد العالمية ليزود مشتري منتجات تكنولوجيا المعلومات بخيار شركاء وباعة التكنولوجيا المعتمدين؛ علماً بأن المجموعة المفتوحة هي التي وضعت المعيار [b-ISO/IEC 20243] المذكور أعلاه لأول مرة.

ويمكن الاطلاع على معلومات أوفى عبر الرابط التالي: <http://www.opengroup.org/getinvolved/forums/trusted>

• **معهد مهندسي الكهرباء والإلكترونيات (IEEE)**

وضع معهد مهندسي الكهرباء والإلكترونيات (IEEE) معياراً لهوية الأجهزة الآمنة وأسلوباً لربط الهوية بالجهاز تخفيريًا، مثل المعيار IEEE 802.1ar – "معيار للشبكات المحلية والحضرية: هوية الجهاز الآمنة".

وكما جاء في الموقع الإلكتروني لمعهد مهندسي الكهرباء والإلكترونيات: "يوصّف هذا المعيار معرفات الجهاز الآمنة (DevIDs) المصممة لاستخدامها كبيانات اعتماد آمنة للاستيقان من الأجهزة قابلة للتشغيل البيئي مع بروتوكول الاستيقان القابل للتوسعة (EAP) وغيره من بروتوكولات الاستيقان والتهيئة المعيارية في دوائر الصناعة. وتسهل الهوية المقيّسة للأجهزة الاستيقان الآمن القابل للتشغيل البيئي من الأجهزة وتبسط نشر الأجهزة وإدارتها بأمان."

ويمكن الاطلاع على معلومات أوفى عبر الرابط التالي: <http://www.ieee802.org/1/pages/802.1ar.html>

• **تشمل الأنشطة الصناعية الأخرى المتعلقة بالتزييف ما يلي:**

– ICC – غرفة التجارة الدولية مكتب استخبارات التزييف

<http://www.iccwbo.org/products-and-services/fighting-commercial-crime/counterfeiting-intelligence-bureau/>

– ICC – فريق مبادرة الأعمال لوقف التزييف والقرصنة بغرفة التجارة الدولية (BASCAP)

<http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/Welcome-to-BASCAP/>

بيليوغرافيا

[b-ITU-T-CI-Portal]	ITU C&I Portal under Pillar 4 keeps updated information on country's C&I regulatory framework http://www.itu.int/en/ITU-T/C-I/Pages/default.aspx .
[b-ITU-T TR-Counterfeit]	Technical Report on Counterfeit ICT device (2015).
[b-IEEE 802.1]	IEEE 802.1 (2009), <i>Standard for Local and Metropolitan Area Networks: Secure Device Identity</i> . – http://www.ieee802.org/1/pages/802.1ar.html
[b-ISO/IEC 15408-1]	ISO/IEC 15408-1:2009, <i>Information technology - Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model</i> .
[b-ISO/IEC 17000]	ISO/IEC 17000:2004, <i>Conformity assessment – Vocabulary and general principles</i> .
[b-ISO/IEC 20243]	ISO/IEC 20243:2015, <i>Information Technology – Open Trusted Technology Provider TM Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products</i> .
[b-ISO/IEC 27034]	ISO/IEC 27034:2011, <i>Information technology – Security techniques – Application security</i> .
[b-ISO/IEC 27036-3]	ISO/IEC 27036-3:2013, <i>Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security</i> .
[b-EC-Regulation]	Market Surveillance Regulation EC no. 765/2008.
[b-Gartner]	https://www.gartner.com/it-glossary/gray-market
[b-ITU-D-CI-Guidelines]	ITU Guidelines on Establishing conformity and interoperability regimes: Complete Guidelines (2015), ITU http://www.itu.int/en/ITU-D/Technology/Documents/ConformanceInteroperability/publications/Establishing_Conformity_and_interoperability_Regimes-E.pdf
[b-ITU-D-Rep]	Final Report for the Question 4/2 – Question 4/2: Assistance to developing countries for implementing conformance and interoperability programmes, ITU-D Study Groups, 2017, https://www.itu.int/pub/D-STG-SG02.04.1-2017
[b-OECD]	2017 OECD report "Trade in Counterfeit ICT Goods".
[b-TRIPS Agreement]	Trade-Related Aspects of Intellectual Property Rights; annex of the Marrakesh Agreement Establishing the World Trade Organization, signed in Marrakesh, Morocco on 15 April 1994.
[b-UNECE]	Recommendation M. on the: Use of Market Surveillance Infrastructure as a Complementary Means to Protect Consumers and Users against Counterfeit Goods. http://www.unece.org/fileadmin/DAM/trade/wp6/Recommendations/Rec_M.pdf
[b-WCO-IPM]	World Customs Organization IPM – http://www.wcoipm.org/
[b-WTO-TBT]	World Trade Organization – WTO Agreement on Technical Barriers to Trade.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريف 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	المطاريق 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 بروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات