الشبكة العربية لهيئات تنظيم الاتصالات وتقنية المعلومات

الاجتماع السنوي السادس عشر للشبكة العربية لهيئات تنظيم الاتصالات

وتقنية المعلومات

المنامة، مملكة البحرين

2-4/ أكتوبر 2018

مشروع تبادل الخبرات في مكافحة تهريب المكالمات الدولية الذي يتم من خلال استخدام أجهزة (SIMBox)

2017-2018

المحتويات

1. المقدمة .....
   1.1. ضباط الارتباط في هذا المشروع لكل دولة .....
2. انواع وطرق الاحتيال في شبكات الاتصالات
3. طرق الكشف عن الاحتيال في شبكات الاتصالات
4. آلية الاحتيال من خلال استخدام اجهزة (SIMBox)
5. أنواع أجهزة (SIMBox)
   5.1. أجهزة SIMBox
   5.2. أجهزة SIMBank
   5.3. أجهزة SIMServer
6. آلية الاحتيال الالتفافي من خلال أجهزة (SIMBox)
7. طرق الكشف عن الاحتيال الذي يتم من خلال استخدام أجهزة (SIMBox)
   7.1. تحليل سجل المكالمات التفصيلي (CDR: Call Details Record)
   7.2. أنظمة مكافحة الاحتيال (FMS: Fraud Management System)
   7.3. استخدام انظمة (TCG: Testing Call Generator)
8. الآثار والمخاطر لاستخدام أجهزة (SIMBox)
   8.1. الاثار الفنية على المستخدمين وشبكات الاتصالات
   8.2. الاثار الاقتصادية والمالية
   8.3. المخاطر الامنية
9. وجهة النظر التنظيمية والقانونية لاستخدام اجهزة (SIMBox).
10. طرق الوقاية من الاحتيال من خلال اجهزة (SIMBox).
    10.1. ضبط أعداد الخطوط الخلوية وتوثيقها
    10.2. ركائز نجاح مكافحة الاحتيال من خلال اجهزة (SIMBox)
11. تجربة الاردن في مكافحة الاحتيال من خلال اجهزة (SIMBox)
12. الملحقات

1 المقدمة

إشارة إلى الاجتماع السنوي الخامس عشر للشبكة العربية لهيئات تنظيم الاتصالات وتقنية المعلومات الذي عقد خلال الفترة 18 – 2017/9/20 في أبو ظبي، الامارات العربية المتحدة تم إقرار مشروع "**تبادل الخبرات في مكافحة تهريب المكالمات الدولية الذي يتم من خلال استخدام أجهزة (SIMBox)**" لما لهذا الموضوع من أهمية حيث أصبحت هذه الظاهرة منتشرة بشكل كبير في بعض البلدان وظهر تأثيرها بشكل جلي على النواحي الفنية والاقتصادية والمالية للشركات اضافة الى آثارها على الامن القومي.

ويهدف هذا التقرير الى التعريف بانواع الاحتيال في شبكات الاتصالات والتطرق بشكل تفصيلي الى الاحتيال الالتفافي (By–Pass Fraud) وكيفية الكشف عنه وآثاره ومخاطرة ووجهة النظر القانونية والتنظيمية وطرق الوقاية منه، اضافة الى الخروج بافضل ممارسات المنطقة العربية المبنية على الخبرات العميقة والمتراكمة في مكافحة الاحتيال الالتفافي (By–Pass Fraud) الذي يتم من خلال انشاء وادراة وتشغيل شبكات الاتصالات غير المرخصة من أجل انهاء المكالمات الدولية بطرق غير مشروعة باستخدام اجهزة وتقنية (SIMBox). وسيجيب هذا التقرير عن الدور الذي يجب أن تلعبه الهيئات التنظيمية، والخطوات التي يجب اتخاذها على المستوى الوطني من أجل مكافحة الاحتيال الالتفافي (By–Pass Fraud)، من أجل المحافظة على الايرادات المتأتية من المكالمات الدولية المنتهية في البلاد، وجودة خدمات الاتصالات الدولية، والبنية التحتية لشبكات الاتصالات.

وقد تم اعتماد هذا المشروع في الاجتماع السنوي الخامس عشر للشبكة العربية لهيئات تنظيم الاتصالات وتقنية المعلومات برئاسة المملكة الاردنية الهاشمية وعضوية اثنتا عشرة دولة وهم كل من: دولة الامارات العربية المتحدة، مملكة البحرين، الجمهورية الجزائرية الديمقراطية الشعبية، المملكة العربية السعودية، جمهورية السودان، جمهورية العراق، سلطنة عُمان، دولة الكويت، الجمهورية اللبنانية، جمهورية مصر العربية، المملكة المغربية، الجمهورية الإسلامية الموريتانية.

1.1 ضباط الارتباط في هذا المشروع لكل دولة

يوضح الجدول ادناه المعلومات الكاملة لضباط الارتباط في هذا المشروع من الدول المشاركة فيه:

جدول رقم (1): ضباط ارتباط المشروع

تسلسل	الدولة	معلومات ضابط الارتباط في هذا المشروع	
		الاسم / الوظيفة	البريد الالكتروني
1	الأردن	عمر تيسير العودات مدير الدائرة الفنية	omar.odat@trc.gov.jo
2	الامارات	نعيم حمدان راشد المعمري	naim.hamdan@tra.gov.ae rashid.almemari@tra.gov.ae
3	البحرين	السيد عادل محمد درويش رئيس إدارة العلاقات الدولية	adarwish@tra.org.bh
4	الجزائر	عدنان لطيفة	l.adnane@arpt.dz
5	السعودية	خالد خليل محمد المعارك	kkhalil@citc.gov.sa mhmaarik@citc.gov.sa
6	السودان	عبد المنعم عوض	moneimam@ntc.gov.sd
7	العراق	وجدان كرم داليا كفاح	d.salim@cmc.iq da91lia@gmail.com
8	عُمان	ناصر الجابري	nasser.aljabri@tra.gov.om
9	الكويت	خالد فالح العازمي	k.alazmi@citra.gov.kw
10	لبنان	كارول حاج	Carole.hage@tra.gov.lb
11	مصر	تامر القزاز	tali@tra.gov.eg
12	المغرب	يونس بنشرقي محمد قرشي	bencherki@anrt.ma korchi@anrt.ma
13	موريتانيا	الشيخ التجاني أداع	Tij.oudaa@are.mr

2 انواع وطرق الاحتيال الرئيسية في شبكات الاتصالات

a) احتيال أنظمة المقاسم الفرعية/البريد الصوتي (PBX/Voicemail Systems)
b) احتيال أو سرقة الاشتراك/الهوية (Subscription/Identity theft)
c) احتيال المشاركة بالعوائد الدولي (International Revenue Share Fraud–IRSF)
d) الاحتيال الالتفافي (By–Pass Fraud)
e) احتيال البطاقات الائتمانية (Credit Card Fraud)

3 طرق الكشف عن الاحتيال في شبكات الاتصالات

4 آلية الاحتيال من خلال استخدام اجهزة (SIMBox)

لم تعط الدراسات العالمية رقمًا دقيقًا حول مقدار الخسائر المالية للحكومات والمشغلين والأضرار التي لحقت بالبنية التحتية بسبب الاحتيال الالتفافي (By–Pass Fraud) الدولي الناتج من استخدام أجهزة (SIMBox) غير المشروعة، كما لم تصدر أي منظمة دولية أو منظمة رقابية (الأمم المتحدة، الاتحاد الدولي للاتصالات ... الخ) أرقاماً رسمية عن الخسائر الناجمة من هذا النوع من الاحتيال.

من جهة أخرى فان شركات الاتصالات والدول التي تصاب بالاحتيال الالتفافي (By–Pass Fraud) الدولي عبر نشاط أجهزة (SIMBox)، تبدو الأعراض لديها واضحة للغاية: فالإيرادات المتأتية من حركة الاتصالات الصوتية الدولية تأخذ في الانخفاض؛ وجودة الخدمة الصوتية للاتصالات الدولية تزداد سوءًا، ويزداد الطلب على الشرائح الخلوية (SIMCard).

ويعتبر الاحتيال الالتفافي (By-Pass Fraud) الدولي عبر نشاط أجهزة (SIMBox) هو أحد أصعب مشاكل الاحتيال التي يواجهها مشغلو الاتصالات على الصعيد العالمي، ويتم انفاق ملايين الدولارات على حلول إدارة الاحتيال سنوياً، وعلى المستوى الوطني، تزداد المشكلة تعقيدًا إذا قام أحد المشغلين في تنظيف شبكته بشكل ممتاز من الاحتيال الالتفافي، فسوف يصعد المحتالون هجماتهم على المشغلين الآخرين في البلاد، لذلك فإن الأثر النهائي هو أن الخسائر والأضرار الاقتصادية لا تزال تحدث في الدولة.

وتتمثل استراتيجية الاحتيال الالتفافي والذي يعتبر أحد اهم أنواع الحروب الالكترونية بما يلي:

أ. خداع أنظمة الكشف:

تعتبر خوادم SIM من اشهر الانظمة الفنية، الذي يمكّن للمحتالين من السيطرة على عمليات الاحتيال الالتفافي من موقع مركزي، حيث لم تعد بطاقات SIM بحاجة إلى أن تكون جسديًا في الشبكة المحلية المصابة ، فقط الهوائيات التي تفرغ حركة المرور الاحتيالية على شبكة الهاتف المحمول المحلية. كم أن هناك مقدرة لتلك الاجهزة خفض استخدام كل بطاقة SIM إلى أدنى حد ممكن، وتسمح بنوك التخزين الكبيرة لبطاقات SIM للمحتالين بتدوير استخدام بطاقة SIM بسرعة وبشكل تلقائي حتى لا ينبه أنظمة FM.

ب. التفريق والغزو

حيث يتم دراسة السوق والبحث عن المشغل الأقل مقاومة لأنواع الاحتيال والعمل على الربط على شبكته، من خلال استخدام بطاقاته داخل انظمة SIMBox ، على الرغم من أن المشغلين الآخرين يقومان بعمل جيد في منع الدخول على شبكاتهما الخاصة ، إلا أن مقدار الالتفاف على المستوى الوطني يبقى كما هو. من جهة أخرى قد يكون هذا المشغل الاقل مقاومة يكسب مالياً من نشاط تجاوز المحتال؛ مثل حركة هاتفية محلية كبيرة تشمل (on-net, off-net)، مبيعات ضخمة في السوق للشرائح الخلوية، زيادة الحصة السوقية، وبالتالي قد لا يكون هناك أي حافز على منع هذا الاحتيال، ومن هنا تأتي اهمية وجود الجهة التنظيمية لكون بعض الشركات تحقق بعض المكاسب من هذا الاحتيال.

5 أنواع أجهزة (SIMBox)

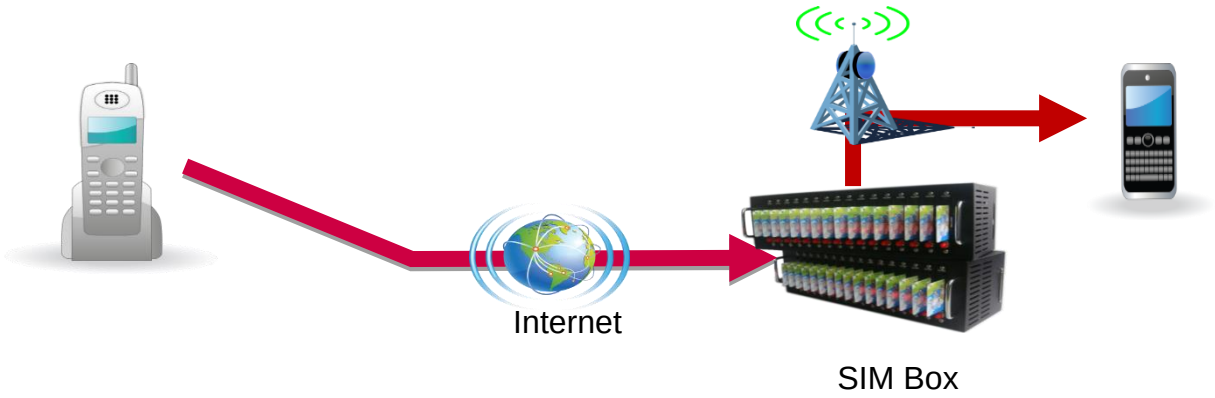
1.1. أجهزة SIMBox

1.2. أجهزة SIMBank

1.3. أجهزة SIMServer

6 آلية الاحتيال الالتفافي من خلال أجهزة (SIMBox)

تعتبر أجهزة (SIMBox) جزء من شبكات الاتصالات غير المرخصة والتي تستخدم في انهاء المكالمات الدولية بطرق غير مشروعة على شبكات الاتصالات المحلية. وبشكل مبسط تتكون شبكة الاتصالات غير المشروعة من جهاز (SIMBox) الذي يكون مربوط من جهة مع شبكة الانترنت من خلال مودم الانترنت بحيث يتم نقل المكالمات لدولية باستخدام تكنولجيا الانترنت (VoIP) الى جهاز (SIMBox) الذي يعمل كبوابة (Gateway) مع شبكات الاتصالات الخلوية بحيث يقوم بانهاء المكالمات القادمة عبر شبكة الانترنت الى شبكات الاتصالات الخلوية من خلال الشرائح الخلوية (SIMCards) الموجودة فيه كما هو موضح أدناه.

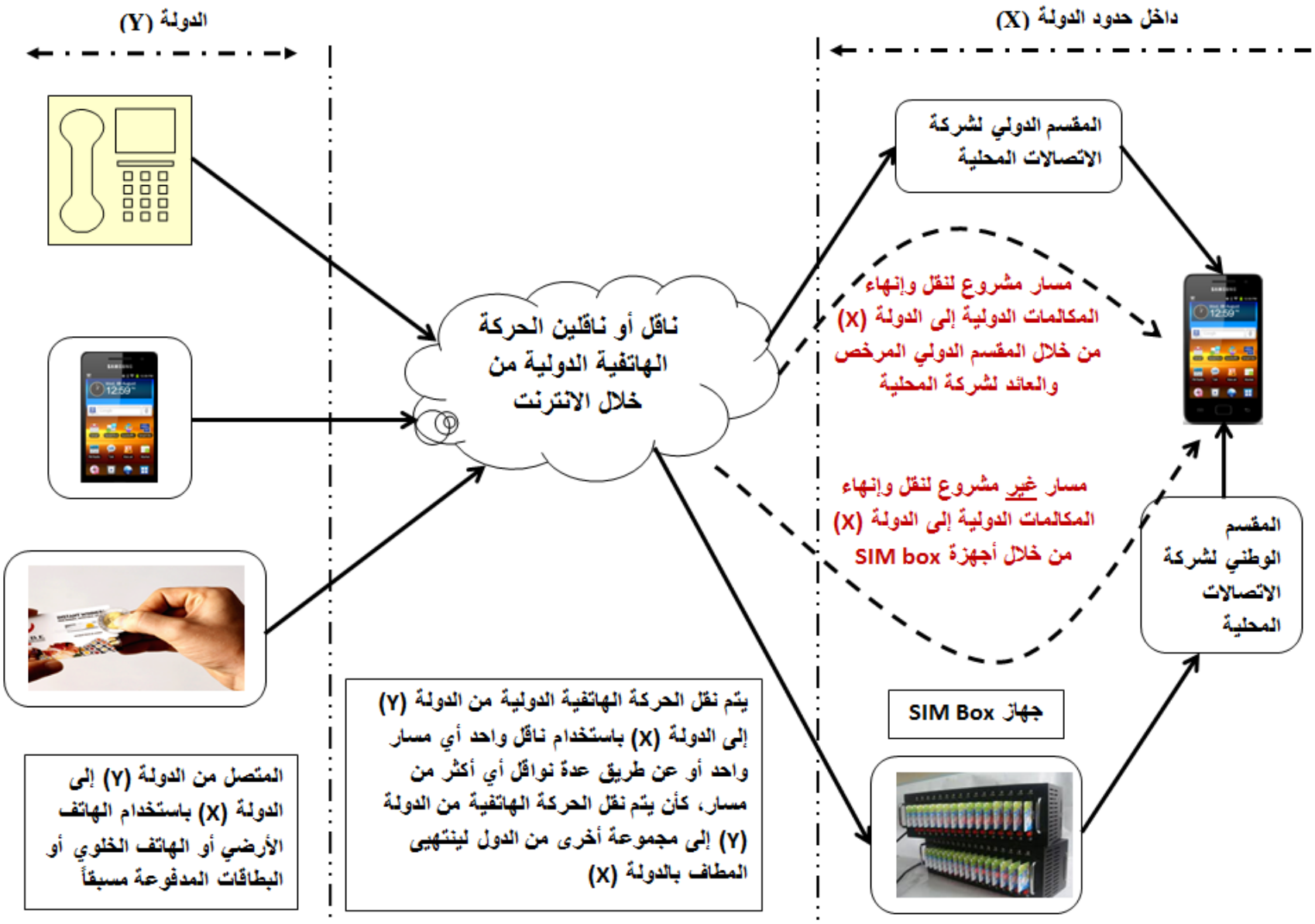


يوضح الشكل التالي مثال لعملية استخدام أجهزة SIMBOX للتحايل على المقاسم الدولية لشركات الاتصالات الخلوية من خلال إعادة توجيه الحركة الهاتفية الدولية ليتم تمريرها كمكالمة محلية من خلال المقاسم المحلية لشركات الاتصالات الخلوية.

وعلى سبيل المثال أن هناك مكالمة صادرة من دولة (Y) – سواء كانت تلك المكالمة صادرة من هاتف ارضي أو من هاتف خلوي أو من خلال بطاقات الاتصال الدولية– حيث تمر تلك المكالمات من خلال ناقل / نواقل الحركة الهاتفية الدولية ليتم إنهاء تلك المكالمة في دولة (X)، وعلى سبيل المثال ليكن الشخص المطلوب مشترك لدى شركة اتصالات محلية.

في حال تم إنهاء المكالمات الدولية إلى المملكة من خلال المقسم الدولي المرخص والعائد لشركة الاتصالات المحلية؛ فان هذا المسار يعتبر **مسار مشروع**، ويقوم ناقل / نواقل الحركة الهاتفية الدولية القادمة من الشركات في دولة (Y) إلى دولة (X)، بدفع ثمن عالي لشركة الاتصالات المحلية مقابل إنهاء المكالمة على شبكتها، (أي يتم محاسبة شركة الاتصالات المحلية على أساس أن المكالمة دولية) إضافة إلى كون المكالمة تكون ذات جودة جيدة ويظهر رقم المتصل من الدولة (Y) ويكون العائد المالي من المكالمات الدولية (International Calls) المنتهية على شبكات الدولة (X) المحلية المرخصة عالي مقارنة مع المكالمات المحلية (National Calls).

في حال تم إنهاء المكالمات الدولية إلى الدولة (X) من خلال أجهزة (SIM Box)؛ فان هذا المسار يعتبر **مسار غير مشروع**، ويقوم ناقل / نواقل الحركة الهاتفية الدولية القادمة من الشركات في دولة (Y) إلى دولة (X)، بدفع ثمن أقل نسبياً للشخص المالك لأجهزة (SIM Box) مقارنة مع ما هو مدفوع لشركة الاتصالات المحلية المرخصة، مقابل قيام هذا الشخص بالتحايل في إنهاء المكالمة الدولية على شبكة شركة الاتصالات المحلية المرخصة من خلال استخدامه لأجهزة (SIM Box) والتي تحتوي على شرائح اتصال محلية (SIM Card) تقوم بربط أجهزة (SIM Box) بالمقسم المحلي لشركة الاتصالات المحلية (أي أن هناك فقدان للمورد من المكالمات الدولية المنتهية على شبكات الدولة (X)) إضافة إلى رداءة الاتصال وعدم ظهور رقم المتصل من الدولة (Y)، ويذهب العائد المادي من المكالمات الدولية للشخص المالك لأجهزة (SIM Box).


الدولة (Y)
داخل حدود الدولة (X)
المقسم الدولي لشركة الاتصالات المحلية
ناقل أو ناقلين الحركة الهاتفية الدولية من خلال الانترنت
مسار مشروع لنقل وإنهاء المكالمات الدولية إلى الدولة (X) من خلال المقسم الدولي المرخص والعائد لشركة المحلية
مسار غير مشروع لنقل وإنهاء المكالمات الدولية إلى الدولة (X) من خلال أجهزة SIM box
المقسم الوطني لشركة الاتصالات المحلية
جهاز SIM Box
يتم نقل الحركة الهاتفية الدولية من الدولة (Y) إلى الدولة (X) باستخدام ناقل واحد أي مسار واحد أو عن طريق عدة نواقل أي أكثر من مسار، كأن يتم نقل الحركة الهاتفية من الدولة (Y) إلى مجموعة أخرى من الدول لينتهي المطاف بالدولة (X)
المتصل من الدولة (Y) إلى الدولة (X) باستخدام الهاتف الأرضي أو الهاتف الخلوي أو البطاقات المدفوعة مسبقاً

7 طرق الكشف عن الاحتيال الذي يتم من خلال استخدام أجهزة (SIMBox)

7.1 تحليل سجل المكالمات التفصيلي (CDR: Call Details Record)

7.2 أنظمة مكافحة الاحتيال (FMS: Fraud Management System)

7.3 استخدام انظمة (TCG: Testing Call Generator)

8 الآثار والمخاطر لاستخدام أجهزة (SIMBox)

تتلخص الآثار والمخاطر الناتجة عن وجود الاحتيال الالتفافي (By-Pass Fraud) الدولي عبر نشاط أجهزة (SIMBox) بما يلي:

8.1 الاثار الفنية على المستخدمين وشبكات الاتصالات

أ. التأثير على جودة خدمات الاتصالات:

هنالك آثار سلبية على مصالح المستفيدين وعدم ضمان لحقوقهم حيث أن خدمات الاتصالات الصوتية الدولية المقدمة من خلال هذه الأجهزة تعتبر ذات جودة اتصالات سيئة للمستخدم النهائي كون المعدات المستخدمة تعتبر رخيصة ومنخفضة الجودة لخفض تكاليفهم ، وبالتالي فأن مكافحة هذه المخالفات يعتبر حماية للشركات والجهات الحاصلة على التراخيص اللازمة وفقاً للقوانين والتشريعات النافذه من جهة، وحماية أيضا لمصالح المستفيدين.

ب. البنية التحتية لشبكات الاتصالات

أظهرت بعض الدراسات العالمية بهذا الخصوص أن انتشار ظاهرة الاحتيال الالتفافي (By-Pass Fraud) الدولي عبر نشاط أجهزة (SIMBox) تعمل على تقليل الايرادات المتأتية من خدمات الاتصالات الصوتية الدولية وبالتالي فان هذه الظاهرة تقلل من الحافز عند شركات الاتصالات في الاستثمار في البنية التحتية لشبكات الاتصالات.

8.2 الاثار الاقتصادية والمالية

أ. خسارة في إيرادات شركات الاتصالات:

ان الاحتيال الالتفافي (By-Pass Fraud) الدولي عبر نشاط أجهزة (SIMBox) يتسبب في خسارة للايرادات المتأتية من خدمات الاتصالات الصوتية الدولية، حيث أن هؤلاء المحتالون يقومون بسرقة جزء من حصة المكالمات الدولية المنتهية في بلد ما، والتي كان يجب أن تنتهي عبر القنوات وطرق الاتصال الرسمية والمشغلين المرخصين، الا أن انتهائها بتلك الطريقة تسبب في خسارة على المرخصين وعلى البلد بشكل عام.

ب. خسارة في الإيرادات الحكومية (الضرائب وحصة المشاركة في العائدات):

حيث أن الخسارة في إيرادات شركات الاتصالات تتسبب في خسائر في الايرادات الحكومية، ومن جهة فان الحكومات لا تعلم عن حجم ايرادلت مشغلي شبكات الاتصالات غير المرخصة باستخدام تقنية (SIMBox).

ج. جرائم اقتصادية

يمكن أعتبار هذه المخالفات المرتكبة كجريمة اقتصادية، لكون أثرها على إيرادات شركات الاتصالات الخلوية وانعكاس ذلك على الاقتصاد والأمن الوطني.

8.3 المخاطر الامنية

وتنطوي تحت استخدام هذا النوع من الاحتيال عدد من المخاطر الامنية منها:

أ. أمن الاتصالات الصوتية:

ان تمرير المكالمات الصوتية بطرق غير مشروعة من والى جهات غير معلومة وغير موثقة ومعروفة يشكل تحدياً في أمن الاتصالات لابد من معالجته،

ب. اختراق خصوصية المستفيدين:

تتمتع الشبكات العامة بالأمان والخصوصية والتشفير المدمج، ولكن المكالمات المرسلة عبر الشبكات الالتفافية تسمح لمشغل تلك الشبكات بالاستماع إلى المحادثات وتسجيلها والاحتفاظ بها.

ج. تجاوز أنظمة الاعتراض المشروعة:

ان المكالمات الهاتفية غير القانونية التي تم إنهاؤها بطرق غير مشروعة تتجاهل أنظمة المراقبة القانونية التي تستخدمها الأجهزة الأمنية لتعقب المجرمين والإرهابيين.

د. اختراق الرسائل القصيرة (SMS):

يتم أيضا اختراق الرسائل القصيرة (SMS) عن طريق ظاهرة الاحتيال الالتفافي (By-Pass Fraud) من خلال أجهزة مخصصة تسمى (SMS Gateway)، وهذ الظاهرة مثيرة للقلق كون خدمة الرسائل القصيرة (SMS) أصبحت قناة اتصال رئيسية للبيانات السرية والشخصية، اضافة الى أن آلية الارسال من التطبيق إلى الشخص (A2P) مثل تلك الموجودة في البنوك ، وشركات الطيران ، وأسواق المستهلكين الاستهلاكية تعتبر منطقة نمو ضخمة تغذيها أنظمة الإعلام المؤتمتة.

9 وجهة النظر التنظيمية والقانونية لاستخدام اجهزة (SIMBox).

من النواحي التنظيمية يمكن تحليل المخالفات المرتكبة من الاحتيال الالتفافي (By-Pass Fraud) الدولي عبر نشاط أجهزة (SIMBox) بثلاث نقاط رئيسية تعتمد ومرتبطه بقوانين الدول:

أ. إنشاء وإدارة وتشغيل شبكة اتصالات عامة وتقديم خدمات اتصالات عامة دون الحصول على التراخيص اللازمة من الهيئة،

ب. استخدام شبكة اتصالات عامة وربط شبكة الجهة المخالفة مع شبكة اتصالات عامة بطريقة غير قانونية ودون وجه حق لتمرير وإنهاء المكالمات الدولية على شبكات الاتصالات المحلية، حيث أن الربط يتم من خلال الخطوط الخلوية (SIM Cards) المخصصة لاستخدام المشتركين وليس لأجل نقل الحركة الهاتفية، حيث أن الشركات المرخصة ترتبط فيما بينه من خلال اتفاقيات الربط البيني عبر خطوط (E1) وأنظمة التشوير (SS7) وليس كما هو مستخدم في الشبكات المخالفة.

ج. إدخال أجهزة اتصالات دون الحصول على الموافقات اللازمة من الهيئة، حيث أنه وفي حال تم التقدم بشكل رسمي للهيئة من اجل ادخال مثل تلك الاجهزة فان الاجراء سيكون رفض طلب الادخال وضبط ومصادرة الاجهزة.

ومن النواحي القانونية فان النصوص القانونية تنوعت حول التعامل مع المخالفات المرتكبة من خلال الاحتيال الالتفافي (By-Pass Fraud) الدولي عبر نشاط أجهزة (SIMBox) فبعض الدول أفردت نص خاص وواضح بهذه الظاهرة ودول اخرى لم تتضمن نص مباشر حول تلك الظاهرة، والجدول التالي يوضح بعض الامثلة على ذلك.

	نوع النص	اسم الدولة
1	نص خاص ومباشر بهذه الظاهرة	مصر
2	نصوص عامة	الأردن

الأردن:

النصوص القانونية ذات العلاقة بضبط هذا النوع من المخالفات بالاستناد الى قانون الاتصالات رقم (13) لسنة 1995وتعديلاته:

المادة 78

أ . كل من انشا او شغل او ادار شبكة اتصالات عامة بهدف تقديم خدمات اتصالات عامة خلافا لاحكام هذا القانون يعاقب بالحبس مدة لا تقل عن ثلاثة اشهر او بغرامة لا تقل عن (5000) دينار ولا تزيد على (25000)

دينار او بكلتا هاتين العقوبتين.

المادة 79

كل من استخدم شبكة اتصالات عامة او خاصة بطريقة غير قانونية او ربط شبكته مع شبكة اتصالات اخرى دون وجه حق او اعاق الخدمات المقدمة من شبكات اتصالات اخرى او عرض المصلحة الوطنية للخطر يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على ستة اشهر او بغرامة لا تقل عن (2000) دينار ولا تزيد على (5000) دينار او بكلتا هاتين العقوبتين.

المادة 82

كل من استورد او تاجر باجهزة اتصالات مخالفة للقواعد الفنية او تحمل بيانات او معلومات غير صحيحة خلافا لاحكام المواد (48) و (49) و (50) و (51) من هذا القانون يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على سنة او بغرامة لا تقل عن (100) دينار ولا تزيد على (2000) دينار او بكلتا هاتين العقوبتين.

المادة 84

بالاضافة الى العقوبات المنصوص عليها في المادتين 78 و79 من هذا القانون، يجوز للمحكمة المختصة بناء على طلب الهيئة ان تقرر الزام المخالف بدفع مبلغ لا يقل عن ضعفي الرسوم التي تستحق على ترخيص تلك الخدمة لو كانت مرخصة كالزامات مدنية لصالح الهيئة.

10 طرق الوقاية من الاحتيال من خلال اجهزة (SIMBox).

10.1ضبط أعداد الخطوط الخلوية وتوثيقها

تؤكد الهيئة على شركات الاتصالات الخلوية والوكلاء والموزعين المعتمدين لديها وعلى نقاط البيع بالالتزام بعدم بيع أية خطوط خلوية (SIM Card) دون توثيقها بالشكل الصحيح عملاً بتعليمات تنظيم ترخيص نقاط بيع خطوط الهواتف المتنقلة لسنة 2015 والصادرة عن وزارة الداخلية، اضافة الى ان العمل جاري على تفعيل أنظمة شراء الخطوط الخلوية (SIM Card) من خلال البصمة، كما ان وزارة الداخلية سمحت للمواطن الاردني بتسجيل ١٠ خطوط باسمه ولغير الاردني ب٣ خطوط؛ حيث انه من خلال هذه الاجراءات يصعب منفذي عملية الاحتيال الالتفافي (By-Pass Fraud) الدولي الناتج من استخدام أجهزة (SIMBox) على تغذية تلك الاجهزة وادامتها بالشرائح الخلوية اللزمة لعملها.

10.2ركائز نجاح مكافحة الاحتيال من خلال اجهزة (SIMBox)

كما أسلفنا فانه على المستوى الوطني، تزداد المشكلة تعقيدًا إذا قام أحد المشغلين في تنظيف شبكته بشكل ممتاز من الاحتيال الالتفافي، فسوف يصعد المحتالون هجماتهم على المشغلين الآخرين في البلاد، لذلك فإن الأثر النهائي هو أن الخسائر والأضرار الاقتصادية لا تزال تحدث في الدولة، كما أن استمرار عمل تلك الشبكات يعتمد على تزويدها بالشرائح الخلوية، وبالتالي فانه يتوجب على هيئات التنظيم النظر لهذه القضية من خلال منظور وطني يعتمد على توحيد الخبرات والادوات في المكافحة.

ست خطوات يجب على المنظمين اتباعها لغايات السيطرة على الاحتيال:

أ. **كتابة القوانين التي تجعل من الاحتيال الالتفافي (By-Pass Fraud) الدولي جريمة،**

حيث أنه في العديد من الدول، لا توجد قوانين تحظر على وجه التحديد استخدام أجهزة (SIMBox)، حيث على سبيل المثال، تكون العقوبات المفروضة على ارتكاب الاحتيال الالتفافي وخرق القوانين خفيفة للغاية، حيث يتم فرض غرامة على مشغلي شبكات الاتصالت غير المرخصة بقيمة 10000 دولار لانتهاكهم. ومع ذلك ، يمكنهم بسهولة كسب هذا المبلغ في غضون بضعة أيام من التشغيل، مثل هذه العقوبات الخفيفة لا تمنع المحتالين من مواصلة عملياتهم.

ب. **اكتساب رؤية وطنية على نشاط احتيال SIMBox:**

تتوفر أنظمة تحليل بيانات متقدمة يمكنها اكتشاف كل SIMBox نظرًا لتنشيطها على شبكة معينة، على الرغم من عدم تثبيت هذه الأنظمة على جميع الشبكات.

ج. **تنسيق استخدام أنظمة وخدمات مورّدي مكافة الاحتيال (FM: Fraud Managment) لدى المشغلين؛**

من حيث قيام المنظمين في تولي زمام القيادة في تنسيق جهود المشغلين المحليين والمتنقلين وتشجيع موارد FM المشتركة كلما أمكن ذلك.

د. **التدقيق على أداء أنظمة مكافة الاحتيال (FM: Fraud Managment) لمشغلي الاتصالات المتنقلة:**

حيث أنه من المفضل أن تقوم هيئات التنظيم بادارة حملات اختبار تجريبية خاصة بها للتحقق من مدى نجاح المشغلين في أسواقهم في تطبيق أنظمة التحكم. والأكثر من ذلك ، يمكن للمنظمين أيضًا جمع وتحليل سجلات بيانات التفويض (CDR) التي يقدمها مشغلو شبكات الجوّال لاكتساب معرفة أعمق لأنماط الاحتيال مع الحفاظ على الخصوصية والطبيعة التجارية للبيانات CDR التي يملكها كل مشغل.

هـ. لا بد من مكافأة أو معاقبة المشغلين لضمان الامتثال لتعليمات وقرارات الهيئة:

لا يمكن وقف الاحتيال الالتفافي إذا كان أحد المشغلين أو اثنين في بلد ما يغش من خلال تشجيع أو غض الطرف عن المحتالين الذين ينهون المرور عبر بطاقات SIM الخاصة بهم.

و. ضبط (Bust up) عمليات الاحتيال الالتفافي:

إن جانب الإنفاذ هو أمر بالغ الأهمية لأنه يحبط ويخيف المحتالين. عندما يكون التطبيق ضعيفًا أو غير موجود ، يتشجع المحتالون لاستثمار المزيد في بلد ما لأن مخاطرهم أقل بكثير.

11 تجربة الاردن في مكافحة الاحتيال من خلال اجهزة (SIMBox)

لدى هيئة تنظيم قطاع الاتصالات في الاردن تجربة طويلة ورائدة في مكافحة الاحتيال الالتفافي (By-Pass Fraud) تعود لبدايات عام 2000 والتي ظهرت مع بداية توفر سرعات انترنت قادرة على حمل رزم الصوت (VoIP Packets) بجودة اتصالات مقبولة لدى الجهة المستقبلة. وتتم هذه من خلال تقنيات مختلفة تعتمد بشكل رئيسي على تمرير المكالمات الهاتفية الدولية من خلال شبكة الانترنت عبر خطوط مستاجرة (Leased Lines) ليتم انهائها على الشبكات المحلية اما من خلال اجهزة (VoIP Gateway) والتي تنهي المكالمات على الشبكات الارضية الثابتة (PSTN) عبر خطوط (PRI)، أو من خلال استخدام اجهزة (SIMBox) والتي تنهي المكالمات على الشبكات الخلوية عبر استخدام الشرائح الخلوية.

وبشكل عام فان الطريقة الاولى تعتبر قديمة ومن السهل ضبط الجهات التي تقوم بهذه الخاصية من خلال قيام شركات الاتصالات الثابتة بمراقبة حركة المكالمات على الخطوط المستاجرة (Leased

Lines) وفي حال وجود رزم بيانات ذات على علاقة بالصوت (VoIP Packets) يتم مباشرة من تحديد موقع الجهات مرتكبة المخالفات من خلال مكان وجود خط (PRI). كما أن عدد الخطوط المستاجرة (Leased Lines) في حينه محدود ومعروف وكلفها مرتفعة وتتم مراقبة جودتها بشكل مستمر نظرا لوجود SLA Agreements، اضافة ايضا الى خطوط PRI.

مع تطور التقنيات ودخول تكنولوجيا الجيل الثالث والجيل الرابع الى سوق الاتصالات الخلوية بالاضافة الى تكنولوجيا (Wi-Max) والتي تعمل على توفير سرعات عالية تكفي لنقل رزم البيانات (data packets) عبر شبكة الانترنت حتى تصل الى اجهزة (SIMBox) والتي تنهي المكالمات على الشبكات الخلوية عبر استخدام الشرائح الخلوية، أصبح من الصعب جدا مراقبة خطوط البيانات (Data Lines) اضافة الى صعوبة عملية تحديد موقع السيم بوكس بدقة عالية نظراً لأنها تعمل عبر شبكات الاتصالات الخلوية والتي تعتمد على مبدأ (Triangulations) في تحديد موقع الاجهزة الخلوية.

ويتم الكشف عن وجود الاحتيال الالتفافي (By-Pass Fraud) والذي يعتمد على اجهزة (SIMBox) في اي شبكة اتصالات خلوية بشكل عام على استخدام تقنية (TCG: Testing Call Generator) حيث يتم بعد ذلك عملية فصل الارقام التي تظهر على تلك الانظمة اوتحديد الموقع وتنفيذ عملية الضبط.

واتبعت هيئة تنظيم قطاع الاتصالات الاردنية نهج مركزي في القضاء على الاحتيال الالتفافي (By-Pass Fraud) من خلال إدارة جهود منسقة بشكل جيد بين فريق الهيئة وشركات الاتصالات المرخصة والجهات الامنية والشركات المتخصصة المتعاقدة مع الهيئة في الكشف عن الاحتيال وفي تحديد موقع شبكات الاتصالات غير المرخصة والغير قانونية للقضاء عليه. وضمن هذا الفريق يتم دمج البيانات الهامة من أنظمة إدارة الاحتيال الخاصة بشركات الاتصالات الخلوية الأردنية بالإضافة إلى البيانات من الانظمة الفنية الموجودة لدى الهيئة ليتم تحليلها والحصول على معلومات ورؤية شاملة ووافية عن أماكن وحجم الاحتيال في كافة انحاء المملكة.

وحسب قانون الاتصالات الأردني فان المخالفات على تلك الشبكات ترتكز على إنشاء أو تشغيل أو إدارة شبكة اتصالات عامة بغرض توفير خدمات الاتصالات العامة دون الحصول على التراخيص المطلوبة

من هيئة تنظيم الاتصالات وربط شبكة الجهة المخالفة بشبكة اتصالات أخرى دون أن يكون له الحق في ذلك لغايات إنهاء المكالمة الدولية على مشغلي الاتصالات في الأردن بشكل غير قانوني.