الأخبار al-akhbar
الاربعاء 2010-11-24 العدد 1275

الاتصالات واغتيال الحريري | إسرائيل وحزب الله و

«جدران الحماية» تهاوت: تل أبيب ترصد لبن

إسرائيل تسمعنا من هواتفنا، وبإمكانها أن ترى تحركاتنا. فقطاع الاتصالات وقع تحت قبضتها. تتحكم به وفق مشيئتها. هذه خلاصة ما ورد أمس في المؤتمر الصحافي الذي عُقد في وزارة الاتصالات لعرض خلاصة ما توصلت إليه الهيئة المنظمة للاتصالات بعد أشهر من عمليات المسح لقطاع الاتصالات اللبناني

حسن عليق

ربما لم يجد رئيس الهيئة المنظمة للاتصالات بالإنابة، عماد حب الله، الكلمات الوافية لشرح ما توصل إليه فريق من التقنيين العاملين في الهيئة، بعد أشهر من المسح لشبكات الاتصالات في لبنان. في المؤتمر الصحافي الذي دعت إليه لجنة الاتصالات النيابية أمس في وزارة الاتصالات، لجأ حب الله إلى الاختصار المشبع بشروح تقنية، بعضها شديد التعقيد، لكنه يوصل الرسالة واضحة: بإمكان إسرائيل أن تفعل ما تشاء في قطاع الاتصالات في لبنان.

فريق التدقيق في الهيئة المنظمة أجرى مسحاً داخل المؤسسات المشغلة لشبكات الهاتف الخلوي والأرضي، وشبكة الإنترنت، إضافة إلى مسح ميداني بدأه من الجنوب، وبالتحديد، من الحدود اللبنانية ـ الفلسطينية.

عرض حب الله صوراً للمواقع التي نشرتها إسرائيل على طول الحدود، من الناقورة إلى مزارع شبعا. هناك، أقامت الاستخبارات الإسرائيلية مراكز للتجسّس والتنصت، تمكنها، بحسب العرض الموثق، من التنصت على المكالمات الهاتفية، وتحديد مواقع جميع الأجهزة الخلوية واللاسلكية، بما فيها الهواتف الأرضية اليدوية التي يستخدمها المواطنون داخل منازلهم. وتظهر الخرائط التي عُرضت أمس أن المراكز الإسرائيلية تغطي كل مناطق الجنوب والبقاع الغربي، وأجزاءً كبيرة من البقاع الأوسط وجبل لبنان. وفضلاً عمّا ذُكر، فإن لبعضها وظيفة أخرى، هي تمكين الاستخبارات الإسرائيلية من الدخول، عبر بثّ المايكروويف، إلى قلب شركات الهاتف الخلوي. فبحسب الخرائط التي عرضها حب الله والمهندسان في الهيئة محمد أيوب وديانا بو غانم، ثمة مواقع إسرائيلية على خط اتصال بصري بمواقع إرسال عائدة لشبكة الاتصالات اللبنانية (راجع الصورة)، تتيح لها التقاط البث اللبناني بكامله، إضافة إلى استخدام هذه الهوائيات اللبنانية التي تؤدي دور المرسل والمتلقي في الوقت عينه، لبث معطيات إلى داخل الشبكة اللبنانية، والوصول إلى قلب الشركات.

إضافة إلى ذلك، كشف مهندسو الاتصالات عن وجود أجهزة إسرائيلية على الحدود تمكّن الإسرائيليين من تقوية بث إرسال شبكة الهاتف الخلوي الإسرائيلية إلى داخل الأراضي اللبنانية، إضافة إلى تقوية بث الإرسال اللبناني إلى داخل الأراضي الفلسطينية المحتلة، ما يسمح لعملاء إسرائيل باستخدام هواتف إسرائيلية داخل الأراضي اللبنانية، وهو ما لا يمكن الأجهزة الأمنية اللبنانية اكتشافه. كذلك تتيح أجهزة التقوية لرجال

علامات انتشار ابراج التجسس الاسرائيلية على الحدود

خريطتان عُرضتا في وزارة الاتّصالات أمس، تظهر الأولى التوزع الجَغرافي لمواقع التجسّس الإسرائيلية على طول الحدود اللبنانية ـ الفلسطينية، من رأس الناقورة، إلى مزارع شبعا. أما الخريطة الثانية، فتُظهر الاصطفاف الذي يربط الشبكة اللبنانية لمواقع الاستخبارات الإسرائيلية وفقاً للآتي: صفاريه ـ دردغيا ـ زرعيت (إسرائيلي)، وصور ـ دردغيا ـ شبعا (إسرائيلي). وأكد خبراء الاتصالات أن هذا الاصطفاف لم يكن نتيجة الصدفة، بل جرى بناءً على طلب الاستخبارات الإسرائيلية لعملائها، وخاصة أن الاتصال بموقع زرعيت الواقع بين تلتين بحاجة إلى زرع محطات إرسال في أماكن محددة داخل الأراضي اللبنانية.

هكذا اخترقت إسرائيل هواتف كوادر من المقـ

في المؤتمر الصحافي أمس، كشف رئيس لجنة الاتصالات النيابية، عضو كتلة الوفاء للمقاومة النائب حسن فضل الله، عن قصة الخطوط الخلوية الثلاثة التي لطالما ردد مسؤول رفيع في المديرية العامة لقوى الأمن الداخلي أن فرع المعلومات كشف تعامل حامليها مع الاستخبارات الإسرائيلية. قال فضل الله إن القصة بدأت عام 2009، عندما عُقد اجتماع ضم رئيس فرع المعلومات العقيد وسام الحسن ورئيس لجنة الارتباط والتنسيق في حزب الله الحاج وفيق صفا، ليسأل فيه الأول الثاني عمّا إذا كان العميد المتقاعد من الأمن العام، أديب العلم، يعمل بصفة عميل مزدوج لحساب جهاز أمن المقاومة. بناءً على سؤال الحسن، نفى صفا ذلك، مؤكداً أن العلم هو أحد الذين يشتبه جهاز أمن المقاومة في تعاملهم مع الاستخبارات الإسرائيلية، مشيراً إلى أن الشبهات ذاتها تدور حول زوجته ح. ص.

بالفعل، أوقف فرع المعلومات العلم وزوجته، ليبدأ معهما عمله في مجال مكافحة التجسس. وفي الجلسة ذاتها بين الحسن وصفا، زود الأول الثاني بمعطيات عن ثلاثة خطوط هاتف خلوي قال إن كوادر من المقاومة يستخدمونها، وأن فرع المعلومات يشتبه في تعامل هؤلاء مع الاستخبارات الإسرائيلية، بناءً على حركة اتصالاتهم الهاتفية. وتضمنت معلومات الحسن معطيات عن أن الخطوط الهاتفية الثلاثة هي خطوط أمنية يستخدمها هؤلاء الكوادر إلى جانب أرقام هواتفهم المعروفة.

وهذه المعطيات كررها مسؤولون من المديرية العامة لقوى الأمن الداخلي وسياسيون من قوى الرابع عشر من آذار، مستخدمين إياها دليلاً على القدرة الإسرائيلية على اختراق الجسم التنظيمي لحزب الله.

وبحسب فضل الله، فإن جهاز أمن المقاومة أولى هذه المعطيات أهمية قصوى، وأجرى تحقيقات معمقة بشأنها، وخاصة لناحية العثور على الهواتف الأمنية التي أظهرت البيانات أن كوادر المقاومة يستخدمونها. ووصلت التحقيقات إلى طريق مسدود، إذ لم يُعثَر على هذه الهواتف. وبناءً على ذلك، أجري تحقيق تقني نفذه محققون من استخبارات الجيش وجهاز أمن المقاومة، بالتعاون مع فنيين من وزارة الاتصالات والهيئة المنظمة للاتصالات. وبحسب المعلومات المتوافرة عن القضية، تبين أن هاتف أحد الكوادر الثلاثة يحوي في

الأخبار
al-akhbar
الاربعاء 24-11-2010 العدد 1275

وسام الحسن

ان... عارياً

الاستخبارات الإسرائيلية استخدام بطاقات هواتف خلوية لبنانية داخل الأراضي الفلسطينية المحتلة، وتظهر بياناتها في الشركات اللبنانية كما لو أن الاتصالات تُجرى داخل الأراضي اللبنانية.

وبعد الجنوب، انتقل حب الله إلى الشركات المشغلة لشبكات الاتصالات. تحدّث عن «التجهيزات والمعدّات والتطبيقات المستوردة بمجملها من شركات أجنبية وغير خاضعة لأي معايير اختيار واختبار». إضافة إلى ذلك، فإن التوظيف يكون من دون الأخذ بالحسبان معايير الأمن الوطني اللبناني، إذ لا يُدقق في تاريخ الموظفين، ولا سيما الأجانب، لناحية علاقاتهم السابقة (أو الحالية) بإسرائيل. إدارياً، تعاني الهيئات والشركات المشغلة لقطاع الاتصالات من عيوب بنيوية، حيث تُدمَج مهمات يفترض فصلها، كمهمات التخطيط والتنفيذ والرقابة. أضف إلى ذلك، تغيّب المعايير المهنية البسيطة التي تحافظ على أمن الشبكات وخصوصيات المواطنين في الوقت عينه. فعلى سبيل المثال، يجري تبادل كلمات السر بين الموظفين. وقد أثبتت التحقيقات أن هذا الأمر أتاح لأحد المدعى عليهم بالتعامل مع الاستخبارات الإسرائيلية تزويد مشغليه بكلمات السر التي سهّلت لهم التحكم بقطاع الاتصالات اللبناني.

هذه العيوب البنيوية في الهيكلية الإدارية للمشغلين في لبنان تمثّل خطراً مضاعفاً على أمن الشبكات، في ظل بعض التقنيات المعتمدة. فكما هو معتمد في كل أنحاء العالم، إن شبكات الهاتف الخلوي تكون متصلة بشبكة الإنترنت لأسباب عدة، بينها تزويد المشتركين بخدمة الإنترنت عبر الهاتف، إضافة إلى السماح للشركات المورّدة للأجهزة وأنظمة التشغيل بتقديم المساندة التقنية عند وقوع أي أعطال أو أضرار بالشبكة. لكن الدخول إلى الشبكات عبر الإنترنت دونه عقبة رئيسية، هي «جدران الحماية» الإلكترونية، التي لا يُسمَح بعبورها إلا بواسطة كلمات سر.

لكن المشكلة الرئيسية التي كشفها مهندسو الهيئة المنظمة للاتصالات أمس هي أن الشركات المورّدة إلى لبنان متعاقدة في معظمها مع شركات إسرائيلية توفّر لها أنظمة الحماية. بمعنى آخر، إن أنظمة الحماية المتوافرة في الشبكات اللبنانية هي إما مصنّعة في إسرائيل، أو أن شركات إسرائيلية يملكها ضباط من الاستخبارات تمكنت من فكّ الشيفرات العائدة لها. وعُرضت في المؤتمر الصحافي أمس مقتطفات من دراسات منشورة في إسرائيل عن تقنيات فكّ الشيفرات وتصنيع أنظمة الحماية واختراقها، إضافة إلى تفاصيل عن الشركات الإسرائيلية الرئيسية في هذا المجال، كشركتي RSA وCHECK POINT.

ومن هذه النقطة، تحدث المهندسون اللبنانيون عن خاصية عمل الهاتف الخلوي، وكيفية تشفيره واحتمالات اختراقه. وشرح حب الله أن لكل هاتف خلوي رقماً تسلسلياً سرياً، وأن لشريحة الخلوي رقمين سريين. وتحدّث عن قدرات إسرائيل في الكشف عن هذه الأرقام، منذ ما قبل عام 2004، مع الأخذ في الاعتبار أن النسبة الأكبر من شرائح الهاتف الخلوي في لبنان كانت حتى عام 2005 من الجيل الأول (V1) التي «يمكن الهواة استنساخها». والاستنساخ يعني تصنيع شريحة أخرى تحمل رقم الشريحة الأصلية وخصائصها ورقميها السريين واستخدامها، بحيث يظهر أن حامل الشريحة الأصلية هو من أجرى مكالمات في أوقات وأماكن محدّدة، من دون علمه.

وأكد حب الله أن كل ما ذُكر هو كناية عن وقائع ثبت للهيئة المنظمة للاتصالات والأجهزة الأمنية اللبنانية أن إسرائيل تمكنت من القيام بها.

وما يسري على الهاتف الخلوي، يسري على الشبكة الثابتة، وخاصة أنها تعتمد في جزء كبير من وصلاتها على الاتصالات الراديوية (microwave)، ما يسهّل عملية اختراقها. وأورد حب الله مثلاً لحوادث جرت خلال حرب تموز 2006، عندما كانت بعض المباني تُقصَف مباشرة عندما يفتح أحد الأشخاص هاتفاً ثابتاً مسجلاً فيها، رغم أن مستخدم الهاتف كان قد مد شريطاً طويلاً لإبعاد جهاز الهاتف عن المنزل المسجل فيه. وهذه العمليات تؤكد أن للإسرائيليين القدرة على الدخول إلى مركز التحكم بشبكة الهاتف الثابت، التي تُظهر مباشرة كل العمليات الجارية على الشبكة.

ولفت حب الله إلى أن السيطرة على الشبكة تمكّن الإسرائيليين، من بين أمور أخرى، من اختلاق اتصالات لم تجر، ومحو بيانات لاتصالات أجريت. في هذا الإطار، أكدت مصادر رفيعة المستوى في قطاع الاتصالات لـ«الأخبار» أن فريقاً تقنياً تابعاً للهيئة المنظمة للاتصالات أجرى تجارب على هذا الأمر، فتمكن من تسجيل اتصالات في قاعدة بيانات شركتي الخلوي، من دون أن تكون هذه الاتصالات قد جرت بالفعل.

وفي المؤتمر الصحافي الذي عُقد أمس، أكد وزير الاتصالات شربل نحاس أنه «لا مجال للنظر إلى قطاع الاتصالات، في بلد يواجه عدوانية دولة لعلها الأكثر تقدماً في العالم في مجال تقنيات الاتصالات والتشفير وحماية الأنظمة، على أنه مجرد قطاع تجاري. فالاتصالات قائمة على أقانيم ثلاثة: تجاري واقتصادي أولاً، لكنه ضريبي واحتكاري ثانياً، ونضيف أنه تقني وأمني ثالثاً». وفي رأي نحاس، فإن «الواجب الوطني يحتّم التعامل مع قطاع الاتصالات على أساس هذه الأقانيم الثلاثة مجتمعة». وأكد نحاس أن الدولة تعمل مع مؤسسات القطاع الخاص، «من تجارية وفنية وعلمية وبحثية، وعليها أن تحتضن هذه المؤسسات الخاصة وأن ترعى وتواكب ارتقاءها إلى مستويات الكفاءة والحصانة المطلوبة التي لم تكن متوافرة إلى حين أخذنا هذه المسؤولية على عاتقنا، ونستمر بتعزيزها مستقبلاً ضمن الإجراءات المتتالية». ولفت وزير الاتصالات إلى أن «إحدى غايات تمديد شبكة الألياف الضوئية، أن تتمكن من نقل المعلومات من شبكة الراديو إلى منظومة أكثر أماناً». وشدد على أن ثمة إجراءات تُعتَمَد لتوفير حماية القطاع من الاختراق الإسرائيلي، واعداً بعقد مؤتمر صحافي للحديث عمّا يمكن كشفه من هذه الإجراءات. ورداً على سؤال، أكد نحاس أن عقد المؤتمر الصحافي أمس أتى تلبية لتوصية من لجنة الإعلام والاتصالات النيابية، معيداً التذكير بما أعلنه مجلس الوزراء من إشادة بتمكن لبنان من الحصول على إدانة الاتحاد الدولي للاتصالات لإسرائيل على الأضرار والخروق التي ألحقتها بقطاع الاتصالات اللبناني.

من جهته، كشف النائب حسن فضل الله أن الاستخبارات الإسرائيلية كانت قد عرضت على المدعى عليه ش. ق. عام 1997 مبلغ 50 ألف دولار أميركي لقاء زرع معدات تمكّنها من الولوج إلى الشبكة اللبنانية في عدد من المحطات. أضاف فضل الله أن الاستخبارات الإسرائيلية عارضت، من خلال عملائها الذين احتلوا مواقع نافذة، قيام إحدى الشركتين المشغلتين للهاتف الخلوي باستيراد أجهزة جديدة، مصرة عبر أحد عملائها على إبقاء الأجهزة القديمة التي بإمكانه التحكم بها.

اختراق شبكة ألفا خلال الحرب

خلال حرب تموز 2006، وفي شركة «ألفا» لتشغيل إحدى شبكتي الهاتف الخلوي، جرت واحدة من أكبر عمليات القرصنة الإسرائيلية، بحسب ما عُرض في المؤتمر الصحافي أمس. حينذاك، لاحظ عاملون في الشركة أن مركز التحكم يُطفأ ويُعاد تشغيله يومياً، من دون أن يكون أحد من العاملين قد أعطى أمراً لنظام المركز لكي يتوقف عن العمل ثم إعادة تشغيله. وبعد مراجعة سجل الدخول، تبين أنه كان قد تلقى أمراً للتوقف عن العمل. احتار فنيو الشركة، ولم يتمكنوا من فهم ما يجري. جرى الاتصال بالشركة الأجنبية الموردة لأجهزة الشركة ونظم تشغيلها. عُزل مركز التحكم، ومُنِع موظفو «ألفا» من دخول النظام. كذلك أقفلت أبواب «الدخول عن بعد» المتصلة بشبكة الإنترنت، التي يستخدمها المورّدون لتقديم مساعدة تقنية لموظفي شركة «ألفا» عندما يتعرض أحد مرافق الشبكة لأعطال لا يكون التقنيون الموجودون في لبنان قادرين على حلّها.

إقفال كل الأبواب لم يوقف ما يجري في الشركة، وخاصة لناحية وصول المخترقين إلى مركز التحكم وسجلّ الدخول. أمام هذا الواقع، توصل التقنيون إلى نتيجة مفادها أن الاختراق جرى بواسطة الوصلات الراديوية، أي عبر الجنوب. وكان المخترق يوقف تشغيل مركز التحكم ثم يعيد تشغيله لمحو آثار ما قام به، وكذلك الأمر بالنسبة إلى وقف تشغيل سجل الدخول. في الخلاصة، دخل الإسرائيليون إلى مركز التحكم، ابتداءً من 13 تموز 2006 حتى 12 آب 2006، من دون أن يتمكن فنيو الشركة أو أولئك العاملون في الشركة الموردة من معرفة ما فعلوه.

تجدر الإشارة إلى أن مركز التحكم (OMC) يتيح لمن يملك قدرة على الدخول إليه تعقب مستخدمي الهاتف الخلوي لحظة بلحظة، وتحديد أماكن وجودهم عند إجرائهم اتصالات أو تلقيهم لها، أو تشغيل هواتفهم وإرسال رسائل نصية. ورجح فنيو وزارة الاتصالات و«ألفا» أن يكون التعقب هو الهدف الرئيسي للاختراق الإسرائيلي خلال حرب تموز 2006.

اومة

داخله نظام تشغيل يتضمن رقم هاتف مستنسخاً عن رقم هاتف خلوي كان العلم قد اشتراه وأرسله إلى مشغّليه.

وما لم يذكره فضل الله أمس، هو ما أكدته مصادر في قطاع الاتصالات عن أن المحققين والتقنيين العاملين معهم أجروا عدة تجارب على الهاتف المشتبه فيه. وأجريت إحدى التجارب داخل شركة «ألفا»، ومن داخل غرفة التحكم بالتحديد. وتبين أن تشغيل الهاتف المشتبه فيه يؤدي إلى تشغيل خطين خلويين مختلفين، أحدهما الخط الذي يستخدمه حامل الهاتف، والآخر هو الذي كان أديب العلم قد سلمه للإسرائيليين. إضافة إلى ذلك، تضيف المصادر نفسها، يُظهر تشغيل الهاتف المشتبه فيه وجود هاتفين اثنين: الهاتف نفسه، وهاتف آخر يحمل رقماً تسلسلياً مختلفاً. وهذه البيانات تَظهر في غرفة التحكم وفي سجلات الشركة، رغم أن الهاتف المشتبه فيه لا يحوي سوى شريحة واحدة (SIM)، كما هي الحال في الغالبية العظمى من الهواتف المستخدمة في لبنان.

أمام هذا الواقع، أجرى التقنيون مزيداً من التحقيقات، فتبين لهم وجود نظام تشغيل داخل الهاتف، زرعه الإسرائيليون عن بُعد، يسمح لهم بالتحكم بالهاتف كما لو أنه هاتفان وشريحتان مختلفتان. ويستخدم الإسرائيليون هذه التقنية لتحديد مكان الشخص المستهدف، والتنصت على ما يتحدّث به عندما لا يجري أي اتصالات، إذ يتصل الإسرائيليون بالهاتف المستنسخ، من دون أن يعرف حامل الهاتف أن اتصالاً قد ورد إليه. وبذلك، يتحول الهاتف إلى جهاز تنصت.

كذلك، تمكن هذه التقنية الإسرائيليين، من بعث آلاف «الرسائل الصامتة» إلى الهاتف، وهي كناية عن نصوص تصل إلى حافظة الرسائل. وهذه الرسائل تتضمن أحياناً برامج تدفع الهاتف إلى البعث برسائل، من دون أن يشعر مستخدم الهاتف بما يجري في هاتفه.

يُذكر أن الأمين العام لحزب الله كان قد أكد في أحد مؤتمراته الصحافية الأخيرة أن ما حُكي عن قضية اختراق إسرائيل لحزب الله بثلاثة من كوادره جرى التحقق منه، «حرصاً على أمن المقاومة بالدرجة الأولى»، مؤكداً أن جهاز أمن المقاومة تثبت من عدم صحة ما يُشاع. ووعد نصر الله بالكشف عن تفاصيل القضية، إلا أن حزب الله لم يعرض هذه القضية حتى يوم أمس.