1

التهديدات

على رغم أن الإنترنت تفتح المجال للهجمات من أي مكان حول العالم، فإن الهجمات التي تستهدف دول مجلس التعاون لدول الخليج العربية غالباً ما تأتي من الدول المجاورة في المنطقة أو من أطراف غير حكومية يرتبط نشاطها بالتوترات والمظالم الإقليمية. وكما هي الحال في أمريكا الشمالية وأوربا وآسيا فإن في الشرق الأوسط عدداً لا يُستهان به من المنظمات القادرة على القيام بعمليات تخريبية في فضائه الإلكتروني. وتشير التقارير إلى أن كلاً من سورية وتركيا وإسرائيل قد استثمرت أموالاً طائلة لتطوير إمكاناتها لشنّ هجمات إلكترونية. وعلى رغم قلة المعلومات حول هذه البرامج، فإن برنامج إيران الخاص بحرب الفضاء الإلكتروني قد حظي باهتمام خاص. وفي ظل المعلومات المتوافرة بصورة عامة، فقد ركز هذا البحث على أنشطة إيران الإلكترونية.

أشار البرنامج الإخباري "فرونتلاين" *Frontline* الذي تبثّه قناة "بي بي أس" PBS الأمريكية إلى أن الحرس الثوري الإيراني قد أسس عام 2005 شعبة متخصصة في حرب الفضاء الإلكتروني، وقد استقطب قوتها العاملة من ثلاث مجموعات قرصنة في إيران، وهي: "أشيانة" و"شابجارد" و"سيمورغ". كما يعتمد هذا الجيش الإلكتروني على مهارات خارجية، وقد أسس شركات خاصة للتوظيف والتدريب واستخدام التقانة.[1]

وفي أيار/ مايو 2010 صرّح مسؤول كبير في الحرس الثوري الإيراني بأن «الجيش الإلكتروني التابع للحرس الثوري قد استطاع اليوم أن يصبح ثاني أقوى جيش إلكتروني في العالم».[2] وعلى رغم عدم وضوح أسس هذا الادعاء، تعتقد شركة الأبحاث الأمريكية "ديفنس تك" أن الشعبة الإلكترونية لديها حوالي 2400 موظف بالإضافة إلى 1200 من قراصنة الإنترنت (الهاكرز) في القطاع الخاص، ويُعتقد أن ميزانيتها السنوية تفوق 75 مليون دولار.[3] وحتى الآن اقتصرت أنشطة إيران في حرب الفضاء الإلكتروني على هجمات ضد مواقع إلكترونية، كتخريب أو حجب مواقع لشركات إخبارية تغطي حركات المعارضة الإيرانية. وفي 19 كانون الأول/ ديسمبر 2009 تعرَّض موقع "تويتر" للمدوّنات لهجمات تسببت بإغلاقه في عدة مناطق من العالم. وقد أعيد توجيه المستخدمين الذين حاولوا دخول هذا الموقع إلى رسالة تقول:

> «تعتقد الولايات المتحدة الأمريكية أنها تتحكم بشبكة الإنترنت وتسيطر عليها، لكنها مخطئة، فنحن بقوتنا نتحكم بالشبكة، لذا لا تحاولوا استفزاز الشعب الإيراني... من منا على قائمة الحظر الآن، إيران أم الولايات المتحدة الأمريكية؟ إننا نضعهم على قائمة الحظر، فاحذروا».[4]

وبعد شهر من هذه الحادثة تعرض محرك البحث الصيني "بايدو" إلى هجوم مشابه، حيث تم تشويه الصفحة الرئيسية للموقع بعبارة مفادها: «تم تأسيس جيش إيران الإلكتروني للاعتراض على تدخلات المواقع الأجنبية والصهيونية في الشؤون الداخلية لدولتنا ونشر الأخبار الكاذبة والمضلّلة».[5] ومن غير الواضح سبب تعرُّض موقع صيني لهجوم من هذا النوع، إلا أن الرد جاء سريعاً من قراصنة الشبكة في الصين، حيث وجَّه الاتحاد الصيني للقرصنة الإلكترونية، وهو جماعة استَهدفت مراراً

مواقع أمريكية في السابق، ضربة انتقامية ضد سلسلة من المواقع الإلكترونية الإيرانية التي اختيرت بشكل عشوائي في هجمات مشابهة، وبثّت الجماعة رسائل على هذه المواقع رداً على تلك المنشورة على موقع "بايدو".[6]

إن تشويه المواقع الإلكترونية أسلوب يتبعه الهواة، وهو أقرب ما يكون إلى التخريب والعبث الصبياني منه إلى الحرب. ومن الخطأ اعتقاد أن هذه الأنماط من الهجمات تعكس القدرات الكاملة التي يتمتع بها النظام الإيراني. ويتضح من التصريحات العلنية أن إيران تدرك أنها موضع استهداف هجمات أكثر تعقيداً، وبالتالي فإنها تعمل على تطوير إمكانات بمقدورها مجاراة هذه التهديدات. وقد علّق مؤخراً وزير الدفاع الإيراني أحمد فهيدي علانية على استعدادات إيران لخوض حرب فضاء إلكتروني قائلاً: «تعد تقنيات المعلومات والاتصالات حالياً في غاية الأهمية لمختلف الدول وعلينا الاستعداد وتجهيز أنفسنا ضد كافة أشكال الحرب الإلكترونية».[7]

وتضع "ديفنس تك" إيران ضمن قائمة أقوى خمس دول في العالم من حيث قدراتها الهجومية الإلكترونية، كما تبيّن لائحة بأنواع أسلحة الفضاء الإلكتروني التي تشكل ترسانة إيران، وتتضمن أسلحة النبض الإلكترومغناطيسي، وأدوات تشويش البيانات اللاسلكية، وأحصنة طروادة الخفية، والفيروسات، والديدان الإلكترونية.

في تموز/ يوليو 2009 صرَّح خبير الدفاع الإسرائيلي، ألون بن ديفيد لقناة "إيه بي سي" ABC الإخبارية أن إسرائيل دأبت من خلال حملة شنتها على الشبكات العسكرية الإيرانية على تخريب أو إتلاف معلومات تتعلق ببرنامج إيران النووي البحثي.[8] كما أفادت تقارير إيه بي سي أن إسرائيل والولايات المتحدة الأمريكية قد بدأتا برنامجاً لتخريب برمجيات وأجهزة اشترتها إيران من الخارج لاستخدامها في البحث النووي.[9] وصرّح مسؤولون إيرانيون مؤخراً أنه قد تم تدمير شبكة من أجهزة التنصت المزروعة في الفضاء الإلكتروني الإيراني بغرض جمع المعلومات حول برنامجها النووي.[10] وفي ظل ازدياد التوتر بين إيران وإسرائيل، من المرجح تصعيد أنشطة الهجمات الإلكترونية بينهما.

ونظراً لحقيقة أن ما يزيد على مئة دولة قد طوَّرت أو تعمل على تطوير قدراتها الهجومية الإلكترونية، فمن المتوقع أن تشكل حرب الفضاء الإلكتروني جزءاً هاماً من كافة الصراعات المستقبلية، كما ستلعب الأسلحة الإلكترونية الافتراضية دوراً قد يكون حاسماً في الحرب الفعلية. وستكون الغلبة للدولة التي تتفوق في حماية فضائها الإلكتروني وتعطيل فضاء أعدائها بعد أن تضمن قدرة جيشها على استخدام تقنية المعلومات وشن هجمات في الفضاء الإلكتروني الافتراضي بما يُحدِث آثاراً ملموسة. وفي هذا الصدد تتمتع الحرب الإلكترونية بقدرة تغيير موازين القوى في الصراعات التقليدية، إلا أن خطراً أكبر قد يكمن في استخدام الهجمات الإلكترونية لأغراض إجرامية. وعلى رغم قوة إجراءات تطبيق القانون في دول الخليج، فإن ذلك لم يحل دون تعرضها لمشكلة الجريمة الإلكترونية.

أشارت مؤسسة "تريندمايكرو" TrendMicro المتخصصة بالأمن أنه خلال عام 2009 تسبب قراصنة الإنترنت بتعطيل حوالي 800 ألف نظام في المملكة العربية السعودية، وأن الدافع وراء معظم هذه الهجمات كان دافعاً مالياً. وفي دولة الإمارات العربية المتحدة تسبب قراصنة الإنترنت بتعطيل حوالي 250 ألف نظام، وفي كلا البلدين تم تعقُّب هذه الهجمات ليتبين أن معظمها قادم من مواقع خارج نطاق الدول المستهدَفة.[11] وفي عام 2008 وقَعت وزارة التربية والتعليم ووزارة العمل في دولة

الإمارات العربية المتحدة ضحية لهجمات تصيُّد كان الهدف منها جمع معلومات شخصية من زوار الموقع، حيث أنشأ متسللو الإنترنت المسؤولون عن هذه الحادثة مواقع مطابقة تقريباً للموقع الرسمي www.moe.gov.ae والموقع www.mol.gov.ae تحت اسم www.mol.gov.tk وwww.moe.gov.tk وهي مواقع مسجلة في إقليم "توكيلاو" في نيوزيلندا.[12]

وفي آذار/ مارس 2010 حذّرت شرطة أبوظبي من ازدياد أنشطة الجرائم الإلكترونية التي تستهدف الأفراد للحصول على معلومات حول حساباتهم المصرفية.[13] قد تكلف الجريمة الإلكترونية الأفراد المقيمين في دول الخليج والشركات العاملة فيها المليارات، الأمر الذي من شأنه أن يقلل من جاذبية المنطقة بالنسبة للمستثمرين الأجانب والمقيمين المحتملين. لذا يجب اتخاذ خطوات موازية لتهديدات الدول لتخفيف تهديدات أنشطة الجريمة الإلكترونية وسد الثغرات أمامها والحد من نتائجها.

نقاط الضعف

هناك عدد هائل من نقاط الضعف في معظم الشبكات المحلية ما يجعل البلدان عرضة لهجمات إلكترونية. وأكثر نقاط الضعف هذه تعد متأصلة في البنية الهندسية للشبكات والبروتوكولات التي تنظم التواصل فيما بينها. وهذا البحث يركز على نقاط الضعف العامة أمام هجمات الحرمان من الخدمة (DDOS) والهجمات على البنية التحتية، والهجمات على الشبكات الحكومية والعسكرية.

هجمات الحرمان من الخدمة

استخدمت روسيا في ثلاث مناسبات مختلفة هجمات الحرمان من الخدمة ضد دول كانت تابعة لها في السابق في أوربا الشرقية وآسيا الوسطى. ففي عام 2007 تعرضت إستونيا لهجمات الحرمان من الخدمة بعد أن أزالت تمثالاً لجندي في الجيش السوفيتي من ساحتها المركزية، وهو نصب تذكاري شيّده الروس خلال مدة احتلالهم للبلد بعد الحرب العالمية الثانية. وفي تلك الحادثة قام قراصنة الإنترنت الروس "الوطنيون" بإغراق الفضاء الإلكتروني للبلد بسيل من ملايين الأوامر والطلبات لصفحات إلكترونية. ولم تقتصر الهجمات على المواقع الإلكترونية، بل استهدفت عناوين بروتوكول الإنترنت الخاصة بالأنظمة الهاتفية والمصرفية.

وبعد سنة ونصف السنة عندما اندلعت أعمال العنف بين روسيا وجمهورية جورجيا، تم استدعاء شعبة الهاكرز الروس للخدمة مجدداً. وقد تزامنت الهجمات الإلكترونية هذه المرة مع الهجمات الفعلية الأرضية والجوية. واستخدم الروس شبكات "البوت" لإطاحة الحكومة الجورجية والمواقع الإلكترونية الإعلامية، وإغراق المجال الإلكتروني للبلاد بزحام خانق بحيث يتعذّر على الحزم الإلكترونية الأخرى دخول البلاد أو الخروج منها. كما سيطر القراصنة على مُوجِّهات الاستقبال للتأكد من التحكم بأي حركة مرور قد تتسرب. وبعد ستة أشهر لجأ الروس إلى هذا الأسلوب مرة أخرى، وكان الهدف هذه المرة جمهورية قرغيزستان في آسيا الوسطى، حيث تم تعطيل الإنترنت في البلد لأكثر من أسبوع.

الهجمات على العمليات الحكومية والعسكرية

تتعرض الأنظمة الحكومية والعسكرية لهجمات يومية في جزء من عمليات التجسس، وتمارس عدة دول هذه العمليات التي تهدف إلى سرقة تصاميم أنظمة الأسلحة أو الحصول على المعلومات المفيدة بسرقة مخططات المعارك، أو فهم طرق تفكير الأعداء المحتملين، أو الإعداد لتعطيل الشبكات وحرمان جيوش العدو من استخدامها في أثناء الحرب. ويعد أي نظام متصل بالإنترنت عرضة للهجوم، كما يعد أي نظام متصل بنظام متصل بالإنترنت عرضة للهجوم أيضاً. لذا قد تجد الحكومات والجيوش التي تعتمد في القيام بوظائفها الرئيسية على هذه الأنظمة أنها غير متوافرة أو لا يمكن الاعتماد عليها عندما تكون في أمسّ الحاجة إليها. وبالتالي فإن ميزة الشبكة العسكرية المتفوقة التي يتمتع بها جيش يتسلح بالتقانة الحديثة قد تذوي وتزول تماماً بفعل الهجمات الإلكترونية.

الهجمات على البنية التحتية الحساسة

مع أن آثار هجمات الحرمان من الخدمة قد تبدو ضئيلة نسبياً من الناحية التقانية فإنها قد تكون مدمرة على الصعيد الوطني، ولا يجوز إطلاقاً الاستهانة بالخسائر الاقتصادية المحتملة التي قد يتكبدها البلد خلال أسبوع من الشلل الذي قد يصيبه جراء انقطاع خدمات الإنترنت عنه. وفي البلدان التي تتمتع بأنظمة عسكرية متطورة تعتمد على تقنيات الشبكة، بإمكان هذه الهجمات أن تقلل من جهوزية تلك الأنظمة وفاعليتها، وغالباً ما تقتصر آثار هذه الهجمات على الفضاء الإلكتروني، إلا أنه في ظل تزايد استخدام أنظمة التحكم الصناعي للإنترنت من أجل تشخيص الأنظمة وإعادة ضبطها وتنفيذ الوظائف الإدارية الأخرى، أصبح بإمكان العابثين والأوغاد الإلكترونيين السيطرة والتحكم عن بعد بوظائف أنابيب الغاز ومرافق إنتاج الوقود والمصانع الكيماوية والمحطات الكهربائية. وفي أي من هذه الحالات قد ينتج عن التلاعب بالبرمجيات المتحكمة في هذه الأنظمة ضرر وإرباك حقيقي على مستوى العالم.

وقد أجرى مختبر أيداهو الوطني التابع للحكومة الأمريكية عام 2006 تجربة أظهرت كيفية تدمير مُولِّد في شركة خدمات عن طريق شن هجوم عبر الإنترنت. وقد تم توصيل المولِّد إلى نظام مخبري بطريقة تحاكي الأسلوب الواقعي المتبع لدى شركات الكهرباء في توصيل الأنظمة، ثم تم الدخول عن بعد إلى نظام المولِّد وإعطاؤه أوامر أحدثت فيه فرقعة وارتجاجاً ثم انفجر من تلقاء نفسه. والجدير بالذكر أن هذه المولِّدات تحتاج ستة أشهر لتصنيعها ويتم إنتاجها حسب الحاجة فقط.

النتائج

إن نتائج أي من هذه الهجمات أمر بديهي، فنظراً لاعتمادنا على التقنيات المتصلة بشبكة الإنترنت بإمكان هجوم الحرمان من الخدمة الذي يستهدف شبكة وطنية أن يصيب بلداً كاملاً بحالة شلل كلية خلال أيام، إلا أن انعكاسات هذا الهجوم قد تدوم لمدة أطول. وفي العقد القادم سيشكل الفضاء الإلكتروني الميدان الذي تبني فيه الدول سمعتها أو تخسرها. فالبلدان التي لا تستطيع ضمان استخدام الإنترنت بشكل مستمر، لن تشكّل أماكن جذب للاستثمار أو العمل أو العيش فيها.

يعتمد اقتصاد منطقة الخليج العربي بشكل أساسي على استخراج ومعالجة النفط والغاز، كما أن مولدات الكهرباء التي تعتمد عادة على النفط والغاز وقوداً تعد ضرورية لاستمرار استخراج ومعالجة الهيدروكربونات. وبما أن هذه المنطقة تعتمد

بشكل كبير على أنظمة التبريد خلال أشهر الصيف الحارة، فإذا تعطلت مولدات الكهرباء هنا فإن قدرة السكان على الاستمرار ستكون موضع تهديد. كما أن محطات تحلية المياه تعتمد على البنية التحتية المولدة للكهرباء وغالباً ما تبنى بجانبها. فإذا ما تعرضت أي من هذه البنى التحتية لهجوم إلكتروني يعطلها فإن النتائج ستكون مدمرة. وأخيراً يمكن القول إن باستطاعة الهجمات الإلكترونية ضد الأنظمة الحكومية والعسكرية أن تقوض قدرة الحكومة في الحفاظ على النظام وتقديم الخدمات المدنية والعسكرية للدفاع عن الحدود الوطنية وإظهار قوتها في الخارج، وستكون التكاليف باهظة في حال عدم معالجة مواضع الضعف هذه.

خطة العمل

مع استمرار ربط العمليات الحيوية بالإنترنت واشتداد شراسة الأنشطة الخبيثة على الشبكات، فإن سلامة الفضاء الإلكتروني للدول ستشكل عنصراً جوهرياً في قرارات الشركات حول أماكن إنشاء أعمالها. وبالتالي فإن الأمن الذي كان يعد مجرد تكلفة يجب تخفيضها سيصبح صاحب الكلمة في السوق. فالبلدان التي لم تحصّن شبكاتها الوطنية من شأنها أن تجتذب المجرمين والمتسللين الإلكترونيين وتحرضهم على ممارسة اعتداءاتهم، ولا يقتصر الأمر على ذلك بل ينال النمو الاقتصادي للبلاد فيعوقه. ولهذه الأسباب يجب على دول مجلس التعاون اتخاذ خطوات لتحويل منطقة دول المجلس إلى "منطقة فضاء إلكتروني آمن وسليم". وكانت الاستراتيجية الوطنية لأمن الفضاء الإلكتروني في الولايات المتحدة لعام 2003 قد اقترحت أمريكا الشمالية لهذا الدور، ولكن هذه الفكرة لم تدخل حيز التنفيذ إطلاقاً. وتعد الإجراءات التالية من أهم العناصر المكونة لمنطقة إلكترونية آمنة:

- تحسين أمن نظام أسماء النطاقات (DNS) في دول مجلس التعاون؛
- التركيز على سلامة الشبكة الوطنية؛
- توطيد التعاون لمعالجة الجرائم الإلكترونية؛
- إعداد خطط تعاونية لتخفيف آثار هجمات الحرمان من الخدمة؛
- تعزيز البنية التحتية الحساسة؛

حماية الأنظمة الحكومية والعسكرية وتحصينها.

الخاتمة

لتخفيف التهديدات وسدّ مواضع الضعف وإدارة النتائج في الفضاء الإلكتروني، على دول مجلس التعاون لدول الخليج العربية التحرك باتجاه اعتماد أجندة موحدة للأمن الإلكتروني. وللمباشرة بهذه الأجندة على دول مجلس التعاون أن تؤسس لجنة توجيهية رفيعة المستوى تضم ممثلين من هيئات تنظيم الاتصالات، ومراكز الاستجابة لطوارئ الحاسب الآلي، والشرطة الوطنية

والجيش، والقائمين على تسجيل النطاقات، ومزودي خدمة الإنترنت، ومشغلي البنى التحتية الحساسة من كل دولة من الدول الأعضاء. وعلى هذه اللجنة بدورها أن تشكل سلسلة من المجموعات الفرعية لمعالجة كل موضوع على الأجندة، بدءاً بتحسين أمن نظام أسماء النطاقات وانتهاءً بتأمين الأنظمة الحكومية والعسكرية. وعندما يتعلق الأمر بجوانب مثل البنية التحتية الحساسة والأنظمة الحكومية والعسكرية، على اللجنة أن تركز فقط على تبادل أفضل الممارسات المتبعة لمعالجة الهموم الأمنية لكل بلد.

أما فيما يتعلق بالجوانب الأخرى كأمن نظام أسماء النطاقات وتحسين وضع الشبكة ومكافحة الجرائم الإلكترونية وتخفيف هجمات الحرمان من الخدمة فيجب تكليف اللجان الفرعية بإعداد خطة استراتيجية مدتها خمس سنوات لتحسين الأمن بشكل ملموس بأسلوب تعاوني. إن الاستثمار البشري والمادي المناسب في هذا الاتجاه من شأنه أن يبدأ بتحسين أمن الفضاء الإلكتروني في دول مجلس التعاون لدول الخليج العربية، مما سيجعل المنطقة مثالاً تحتذي به بقية دول العالم.