مركز الملك فيصل للبحوث والدراسات الإسلامية
King Faisal Center for Research and Islamic Studies

دراسات

ربيع الأول ١٤٣٨هـ
ديسمبر ٢٠١٦م

حل شفرة نشاط إيران الإلكتروني

جاك كارافيلي & سيباستيان ماير

حل شفرة نشاط إيران الإلكتروني

جاك كارافيلي & سيباستيان ماير

جاء استخدام البرمجيات الخبيثة من قِبل الفاعلين من الدول والأنظمة؛ ليغيِّر واقع الهجمات الإلكترونية، ويعلمنا التاريخ أن الدول تستخدم الأسلحة التكنولوجية عند توافرها.

ربما يواجه العالم اليوم سباقاً تكنولوجيّاً خطراً يتسم بظهور الأسلحة القاتلة، ويرى كلاوزفيتز أنه في الحرب تكون اليد العليا للدفاع. ولكن يقلب المجال الإلكتروني هذه المعادلة، ويُوفِّر أيضاً إمكانية لخلق الضبابية التي تتصف بها الحروب من خلال التأثير في الاضطرابات والخداع والارتباك والمفاجأة. لقد بدأنا للتو فقط نتصوّر إمكانات مختلف أشكال البرمجيات الخبيثة والاستراتيجيات والتكتيكات المستخدمة[١].

(1) James P. Farwell and Rafal Rohozinski (2012) "The New Reality of Cyber War", Survival, 54:4, 114.

ح مركز الملك فيصل للبحوث والدراسات الإسلامية، ١٤٣٨هـ

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

كارافيلي، جاك

حل شفرة نشاط إيران الإلكتروني / جاك كارافيلي؛ سيباستيان ماير - الرياض ، ١٤٣٨ هـ

٣٢ ص ؛ ١٦,٥ x ٤٠ سم

ردمك: ٧-٢٨-٨٢٠٦-٦٠٣-٩٧٨

١- إيران - الأحوال السياسية - العصر الحديث ٢- إيران - العلاقات الخارجية أ. ماير، سيباستيان (مؤلف مشارك) ب. العنوان ج. السلسلة

ديوي ٣٣٧,٥٥ ١٤٣٨/٩١٩٨

رقم الإيداع: ١٤٣٨/٩١٩٨

ردمك: ٧-٢٨-٨٢٠٦-٦٠٣-٩٧٨

المحتويات

ملخص

تستكشف هذه الورقة البحثية التطبيقات الموضوعية للحقائق والحسابات المحيطة ببيئة النظام الإلكتروني الإيراني متسارع النمو. كما تستقصي حالات متعددة ترتبط بشدة بالتدخل الإلكتروني من قبل الجمهورية الإسلامية؛ إذ يبذل الجناة جلَّ طاقتهم للتنصّل من المساءلة في النهاية.

وتتضمن نتائج البحث سرداً معمقاً للعواقب الاستراتيجية والتقنية لفيروس ستوكسنت، وهو فيروس غربي الصنع أصاب منشأة نطنز النووية عام ٢٠٠٩م، ثم توجز الورقة الدروس المستفادة من تجربة تلك المنشأة من المنظور الإيراني، بإلقاء الضوء على جهود تطوير النشاط الإلكتروني في البلاد، وذلك في محاولة لتنظيم الموارد المحدودة لجعل إيران فاعلاً رئيساً ومنافساً في الدوائر الإلكترونية العالمية.

وأخيراً، تتناول الورقة التحول الاستراتيجي لإيران بعد (ستوكسنت)، وانتقالها من مجرّد شنّ حملات للتشهير إلى ممارسة عمليات تخريب إلكتروني واسعة النطاق. وقد نتج من هذا التحول القيام بعمليات تدخل متكررة -سواء مباشرةً أو عبر وسطاء إقليميين- تهاجم من خلالها كلاً من الشرق الأوسط والولايات المتحدة وأوروبا منذ ٢٠٠٩م، وحتى الآن.

١- التأثير الممتد لـ(ستوكسنت)

منذ منتصف التسعينيات على الأقل وحكومة الولايات المتحدة تراقب تطورات البرنامج النووي الإيراني بحذرٍ بالغ. وقد تمحور جزء منه حول تعاون إيران مع عدد من الدول مثل: روسيا والصين وكوريا الشمالية وباكستان؛ لتطوير برنامجها النووي والتسليحي. وقرر الرئيس بيل كلينتون انتهاز فرصة تحسُّن العلاقات الأمريكية – الروسية، بعد انهيار الاتحاد السوفييتي؛ للتواصل مع الرئيس بوريس يلسين في محاولة لوقف المساعدات العلمية والتقنية الروسية عن إيران.

ونتيجةً لذلك؛ بدأت جهود دبلوماسية، بقيادة عضو مجلس الأمن القومي جاك كارافيللي؛ للتفاوض حول السبل الممكنة للتخفيف من وطأة المشكلة. ولكن نجاحها كان جزئياً فقط، وأدت إلى اتخاذ إجراءات ضد الجهات الروسية المعروفة بدعم الجهود الإيرانية في هذا الصدد.

وبعدما غادر كلينتون كرسي الرئاسة، استمرت إيران في تطوير برنامجها، وهو ما كان بمنزلة ناقوس خطر في أوروبا وبعض دول الشرق الأوسط أيضاً. وبدأت المفاوضات المباشرة مع إيران مع الثلاثي الأوروبي (بريطانيا وفرنسا وألمانيا)، وانضمت إليهم الولايات المتحدة لاحقاً في مسعى لتحجيم مخاطر النشاط الإيراني.

لم تحرز هذه المحادثات تقدماً سريعاً ملموساً؛ مما دفع مجلس الأمن القومي إلى إصدار سلسلة من القرارات تفرض حزمة من العقوبات على جهات إيرانية مختلفة من مؤسسات وأفراد. واستمرت العقوبات الأمريكية، وأضافت أوروبا حزمةً أخرى من العقوبات الاقتصادية.

وعلى الرغم من كل هذه الإجراءات، فقد أصبح الأمر يمثل تهديداً بصورة أكبر مع بداية فترة الرئيس باراك أوباما أكثر مما كان عليه مع فرض عقوبات دبلوماسية واقتصادية. وألحت حكومة إسرائيل على طلب اللجوء إلى الحلول العسكرية؛ لوقف التقدم النووي وتعاظم التسلح الإيراني.

عارض أوباما هذا الاستخدام «المتطرف» للقوة العسكرية الأمريكية؛ فقد أراد الرئيس الأمريكي -مثله مثل سلفه جورج دبليو بوش- موقفاً أقل عنفاً من استخدام القوة

العسكرية، ولكن بممارسة ضغوط دبلوماسية أشدّ؛ مما مهَّد لصدور قرار باستخدام أول هجمة إلكترونية ضد هدف إيراني، وبالتحديد ضد أجهزة الطرد المركزي التي تُخصِّب اليورانيوم في مفاعل نطنز.

أصدرت (ويكيليكس) في منتصف شهر يوليو من عام ٢٠٠٩م مذكرةً سريةً تفيد باعتقال مخبر إيراني على خلفية واقعة حدثت في منشأة نطنز النووية قبل تسريبها بفترة وجيزة. وفي وقتٍ متزامن، أعلنت هيئة الإذاعة البريطانية (بي بي سي) عن استقالة غلام ريزا أغازاده رئيس هيئة الطاقة النووية الإيرانية. وحتى ذاك الوقت، كانت هناك شكوك حول أنشطة سرية في إطار برنامج منع الانتشار الذي كان يُدار على مدى سنوات بواسطة المخابرات الغربية ضد إيران.

وما ظهر لاحقاً، وأُطلق عليه فيروس ستوكسنت، ربما كان جزءاً مما كان يُعدُّ حينها أكبر مناورة خفيّة لاستخدام المجالات الكهرومغناطيسية (عملية الأولمبياد)، والتي اختارت فيروس ستوكسنت كإحدى برمجياتها الخبيثة؛ لتصيب مفاعل نطنز، وتستهدف أهم البُنى التحتية في إيران، مثل شبكات الكهرباء، والمواصلات العامة، وأنظمة الدفاع الجوي[٢].

ربما تأسَّست هذه الأنشطة السرية بوصفها بديلاً حال فشلت الدبلوماسية الإيرانية – الغربية في التوصل إلى اتفاق بشأن برنامج إيران النووي، وكذلك لتحاشي (الخيار العسكري) المتمثل في ضربة جوية استباقية إسرائيلية أو أمريكية[٣]. وضمَّ المجال العملياتي كذلك جهوداً أخرى لعرقلة الطموح النووي الإيراني أو تأجيله، ومنها الاستهداف المباشر بالقتل. وعلى سبيل المثال، لقي مصطفى أحمدي روشن العالم النووي الإيراني الذي يعمل في منشأة نطنز، حتفه في انفجار قنبلة مغناطيسية في سيارة

(٢) اكتشفت دودة أخرى باسم (دوكو) عام ٢٠١١م، وقد صُممت لجمع المعلومات، وليس التدخل في العمليات الصناعية، على عكس ستوكسنت التي يُعتقد أنها ترتبط به. وشهد عام ٢٠١٢م اكتشاف دودة أخرى منبثقة عنها تحت اسم (فلام) يُزعم استخدامها في عمليات التجسُّس الإلكتروني في الشرق الأوسط بشكلٍ عام، وليس في إيران فقط.

(3) David E.Sanger and Mark Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict", *The New York Times*, February 16, 2016. https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html?rref=collection%2Ftimestopic%2FStuxnet

مفخخة عام ٢٠١٢م[٤]. وعُثر على مجتبى أحمدي الذي يعدُّ أحد أبرز الأسماء في عالم الدفاع الإلكتروني، وأحد قيادات الجيش الإلكتروني الإيراني، قتيلاً في منزله شمال غرب طهران عام ٢٠١٣م.

وهنا يجب وضع عواقب استخدام فيروس ستوكسنت وانتشاره في الحُسبان. وتخبرنا بيانات الوكالة الدولية للطاقة الذرية بأن عدد مراكز التخصيب العاملة في إيران قلّت بشكلٍ ملحوظ منذ ربيع ٢٠٠٩م، على الرغم من تدشين المزيد من أجهزة الطرد المركزية. وجاءت أحداث ربيع ٢٠٠٩م لتحدّ –ربما– من قدرات برنامج التخصيب الإيراني، ونتج منها تأجيل لطموحات إيران النووية نحو عام كامل. وكما تبيَّن لاحقاً، فقد نجح (ستوكسنت) في إبطال مفعول الجهاز المركزي بطريقة توحي بوجود عيوب في التصميم أو في المواد المستخدمة، وليس بأنه هجوم إلكتروني مُتعمَّد.

وتعدُّ أجهزة الطرد المركزية أدوات مُعقدة عالية الدقة تتطلب تحكماً منضبطاً في الفراغ والسرعة وكمية الغاز المستخدم. ويجب ربط آلاف من أجهزة الطرد لتحقيق مستويات التخصيب المرجوة للمواد الذرية القابلة للانشطار. ويظهر تحليل ستوكسنت الآن تفصيلات مثيرة للاهتمام؛ فقد بدا أن جزءاً من البرمجيات الخبيثة التي ضربت أجهزة التحكم تم توزيعه على الكثير من أجهزة الحاسوب الفردية؛ ليتزامن إضراره بتلك الأجهزة معاً؛ ومن ثمَّ يتوسَّع تأثيره. وبما أنه تم تزويد كل جهاز تخصيب بجهاز حاسوب تحكمي صغير مفصل؛ فقد تزامن تشغيل الباراميترات (الوسائط) عمداً؛ مما صعّب من مهمة تحديدها على منصات المراقبة.

وصارت الحواسب الآلية الآن تتحكم تماماً في الأنظمة واسعة النطاق؛ مما يجعل المجمعات الصناعية والمعامل عرضةً للاستهداف والتلاعب. وتعمل سلاسل التزويد المتكاملة في مصافي التكرير أو مصانع الكيماويات أو مصانع الطاقة النووية بالحاسوب، سواءً جزئيّاً أو كليّاً، بشكلٍ مستقل، وبطريقة تبقي درجة الحرارة والضغط والتراكيب

(٤) على عهدة الجارديان، حتى عام ٢٠١٢م كان مقتل روشن خامس حادثة تستهدف علماء إيرانيين منذ عام ٢٠١٠م.
https://www.theguardian.com/world/2012/jan/14/iran-accuses-us-britain-scientist
وللمفارقة، يقال إن إيران نفسها تستخدم الأساليب ذاتها ضد معارضي النظام؛ فقُتل محمد حسين طاجيك القائد السابق لفيلق القدس، وهي وحدة قوات خاصة تابعة للحرس الثوري الإيراني، على خلفية اتهامات بالتجسُّس وتسريب معلومات أمنية لنشطاء من التحرك الأخضر.

في توازن ثابت وقابل للتحكم. وينطبق الشيء ذاته على برامج المراقبة التي تُنظِّم تبريد المواد الجديدة وتزويدها. وعملياً، تعمل الحواسب الصناعية على أنظمة S-٧ متضمنةً أدوات الأتمتة (التشغيل الآلي)؛ بوصفها دعماً لتعديل ومراقبة المستشعرات مثل: ميزان الحرارة الإلكتروني، وصمام التحكم، وسرعة المحرك، ومضخات تبريد المياه.

إن وجود مثل هذه المستشعرات في قلب مفاهيم الأمن الصناعي يسمح بحدوث كوارث حقيقية؛ فلقد نجح هجوم ستوكسنت في تأثيره المدمر بدقة؛ إذ استُهدف تنزيله بسرية كبرنامج مناوراتي في قلب المتحكمات الصناعية أو ما يطلق عليه نظام التحكم الإشرافي وتحصيل البيانات (سكادا).

وبوضع الجهود الضخمة التي بُذلت في تصميم (ستوكسنت) في الحسبان؛ يكاد يكون من المستحيل عزو ابتكاره إلى أصحابه من الأفراد مثل محترفي الجرائم الإلكترونية. وإضافة إلى ذلك، استتبع المواظبة على شراء مثل هذه المكونات عالية الجودة والكفاءة تكلفة عالية لا تقدر على توفيرها إلا الجهات الحكومية أو الممولة من الحكومة.

وضمن (ستوكسنت)، من عدة أوجه، أن يكون توزيعه غير ملحوظ، ويمكن الاعتماد عليه؛ إذ أشار البحث المكثف أن الفيروس يمكنه أن يستخدم طبيعته المناوراتية في نوع واحد فقط من المنصات، وهي المنشآت الصناعية التي تستخدم نظام سيمنز. ولم يحدث ضرر قط في الأنظمة الأخرى، على الرغم من إصابتها بنفس فيروس حصان طروادة. وبنظرة عامة، يمكن القول إن مصممي الهجوم كانوا على دراية دقيقة ببنية النظام والبرامج المستخدمة؛ إذ إنه من دون معرفة وثيقة بالتصميم ونمط التفاعلات بين مكونات S-٧ لم يكن لمثل هذا الهجوم أن يرى النور.

ولذلك؛ تكون الدول فقط هي القادرة على استخدام الموارد مثل: جمع المعلومات الاستخباراتية، والقيام بالاختبارات الدقيقة على سلاح إلكتروني تطفلي؛ لجعله غير قابل للكشف والتحديد.

ويكشف البحث الدقيق عن الإشارات الصغيرة والصلات المؤقتة دلائلَ ظرفيةً عن التصميم والبنية الداخلية لـ(ستوكسنت). وفي سبتمبر ٢٠٠٩م، كشف سيمانتك أن نحو ٦٠ في المئة من الأجهزة المصابة كانت داخل إيران. ويبدو أن (الدودة) كانت مبرمجة بطريقة

كانت ستوقف انتشارها آلياً في يناير ٢٠٠٩م. والمثير للاهتمام أن الأجهزة التي لم يكن فيها التاريخ منضبطاً -وهو التفصيل الذي ربما يبدو غير ذي صلة؛ إذ يستخدم الضبط غير الصحيح للتاريخ عمداً أحياناً للتحايل على تاريخ انتهاء رخص البرمجيات- ظلت متأثرة، حتى تم أخيراً اكتشاف الدودة. وفي نهاية المطاف تأثرت الأنظمة الإلكترونية في نحو ١٥٠ دولة حول العالم بهذا الفيروس(٥).

وقد عُرِفت حقيقة استخدام إيران لأنظمة سيمنز للتحكم الصناعي بصفة دورية بعد اعتراض بضائع مستوردة كانت متجهةً إلى بعض الموردين من قطاع الصناعات النووية الإيرانية. واتضح أن استخدام أنظمة التحكم الصناعي يمكن أن يؤدي إلى تبعات كارثية ذات أهداف تخريبية. وفي مارس ٢٠٠٧م، أطلق فريق من مختبر إيداهو الوطني هجوماً حاسوبياً لأغراض علمية دمَّر عمداً مولداً كهربائياً داخل المختبر.

وانتشر تسجيل مرئي لهذه المحاولة في سبتمبر من العام ذاته، أسفر عن حالة هلع بالنظر إلى هشاشة البنية التحتية في الغرب. ولا يمكن استبعاد أن فكرة تدمير برنامج إيران للتخصيب باستخدام هجوم حاسوبي نبعت أولاً من الدروس المستفادة من (إيداهو).

ولكن يبقى السؤال: كيف حصل المهاجمون على المعرفة والخبرة اللازمة لبدء الهجوم، خصوصاً طرق الوصول إلى البرامج؟

أدى تحليل حجم التخريب الناجم عن (ستوكسنت) إلى معلومات دقيقة عن البنية التحتية المستهدفة. ويمكن تصور أن إيرانياً هارباً أعطى المعلومات المطلوبة للجناة. وفي الوقت ذاته، لا يمكن استبعاد أن يكون الحصول على المعلومات قد تم بعملية سرية على الأرض؛ ممَّا يغذي فرضية أن العامل البشري في تجميع المعلومات الاستخباراتية لا يزال جزءاً محورياً.

ويشير تحليل الحمض النووي غير التقليدي لـ(ستوكسنت) -مع الأخذ في الاعتبار كيف انتشر في أنظمة بعينها فقط- إلى أن المهاجمين كانت لديهم إمكانية توصيل ناقل متسلسل عام (يو إس بي) مصاب إلى النظام المستهدف. وعلى أسوأ افتراض، قد يكون

(٥) للمزيد: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

الجاني بالفعل قد تمكن من سرقة المخطط وتفاصيل الإعداد في مفاعل نطنز؛ إذ لا يمكن الوصول إلى نظام التحكم في نطنز من دون الحصول على معلومات دقيقة من قلب القطاع الصناعي الإيراني لتطوير هذه الشفرة الخبيثة.

وألقت تبعات هذا الهجوم الضوء على أمرٍ مهم، وهو أنه لا يمكن بعدَ الآن حصر العوامل المستقبلية لتقييم أمن النظم والمؤسسات النووية بمدى سُمك الخرسانة المسلحة؛ فأضعف نقطة كانت هي البنية التحتية الداخلية للنظام المعلوماتي الإلكتروني.

وبهذا؛ يمكن الذهاب بفرضية أن الأسلحة الإلكترونية ستستهدف بالتساوي إعاقة قدرة الخصم على تنسيق إجراءات مضادة مناسبة عند اكتشاف الهجوم. ونجح (ستوكسنت) نجاحاً باهراً في خلق فوضى، ودفع الإيرانيين إلى عدم الثقة بأجهزتهم؛ فالفكرة كانت في اللعب مع أفضل العقول العلمية في إيران، وجعلهم يشعرون بأنهم غير مؤهلين للتعامل مع هذه القضايا[٦]. وإلى جانب التبعات التقنية -مثل التسبب في إنهاك الموارد، والإسهام في عرقلة تقدم البرنامج النووي الإيراني- كان (ستوكسنت) يستهدف أيضاً العامل النفسي؛ فحرمان العاملين من التحكم والتسبب في فقدان الثقة بالقدرة التشغيلية للتعامل مع مثل هذه الأزمة يمكن تبريرهما بعدم وجود مخزون من الخطة الاستراتيجية الواضحة. ويرجع الفضل إلى مطلقي (ستوكسنت) في توظيفه بأفضل شكل للاستفادة من إمكاناته.

٢- المركزية والمهنية في إيران ما بعد (ستوكسنت)

عجَّلت تسريبات الولايات المتحدة وإسرائيل بخصوص (ستوكسنت) -بوصفه جزءاً من هجمة إلكترونية أكبر وغير معروفة في هذا الوقت أطلق عليها لاحقاً (عملية الأولمبياد)- بنداء استغاثة لجميع الإيرانيين. ومنذ ذلك الحين وسّعت إيران من قدراتها الإلكترونية، ودعّمت من سمعتها ذائعة الصيت كأحد أفضل الفاعلين الإلكترونيين عالميّاً.

وقدّمت هذه التسريبات لإيران فرصة لعزو التخريب الإلكتروني الذي شاب بنيتها التحتية النووية إلى أعدائها الدائمين؛ الولايات المتحدة وإسرائيل، وإدراك مكامن الضعف، وتحديد الفجوات في القدرات؛ ومن ثمَّ التعلم من الدروس باستخدام مقاربات

(6) James P. Farwell and Rafal Rohozinski (2012) "The New Reality of Cyber War", *Survival*, 54:4.

الهندسة العكسية، وتوليد خوارزميات متشابهة بهدف إطلاق هجماتها هذه المرة؛ ففي النهاية يمكن لإيران الشروع في تصميم ضربات مضادة أعقد وأكثر تكراراً، وتنفيذها برفض دولي أقل وطأة.

لقد طوَّرت إيران بنيتها التكنولوجية التحتية بشكل كبير، وجعلتها أكثر احترافيةً، وتبنت طموحاً سيئ السمعة للتحكم في بيانات الإنترنت الدولية للمستخدمين المحليين باستخدام مقاربة التقسيم؛ وبهذا "تطور النظام الإيراني بشكلٍ ملحوظ عبر استغلاله للفضاء الإلكتروني كوسيلة للقمع الداخلي"، كما برهن على "قدرة متزايدة على وضع أهداف غربية تحت التهديد في الفضاء الإلكتروني؛ وبذلك يصنع بعداً جديداً في النزاع غير المتماثل"[٧].

ومثل كل الدول التي تشهد قيوداً على حرية التعبير والوصول إلى المعلومات، لجأت إيران، مراراً وتكراراً، إلى تمجيد الميزات المزعومة لتمرير اتصالات دولية مركزية لمجموعة محدودة من البوابات محليّاً. وقُدِمت هذه الخطط كحقائق من خلال (خطة التطوير الخمسية الخامسة لجمهورية إيران الإسلامية) من ٢٠١٠م إلى ٢٠١٥م، والتي تتطلب تكوين (شبكة معلومات قومية) تخدم الحكومة الإلكترونية، وتضمن اتصالات آمنة بين الأجهزة الحساسة من حكومة ووزارات وشركات وجهات عسكرية. ومن بين نتائج أخرى متعددة، ظهر هناك رفض مباشر للغرض الأصلي للإنترنت، وهو تبادل المعلومات وتوفيرها للجميع. وتعد هذه المقاربة تحدياً مباشراً لجميع المجتمعات السلطوية.

ونتيجة لذلك؛ تسمح شبكة المعلومات القومية للنظام الحاكم بضمان التحكم في العمليات الدقيقة بشكلٍ مستقل من خلال التقسيم المتعمد لحركة البيانات. وإضافة إلى هذا، تتمكن السلطات الإيرانية من تجاوز عطب مواقع الإنترنت من الشبكات العامة إلى الشبكات الخاصة وفلترة الخدمات من خلال بروتوكول (ميثاق) نقل النص التشعبي (الفائق) HTTP واعتراض المرور عن طريق الوكالة proxy الشفافة أو السرية؛ بناءً على مصدر البيانات، سواء أكان من إيران أم من خارجها[٨].

---

(7) Ilan Berman, "The Iranian Cyber Threat Revisited," Statement before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Washington, DC, March 20, 2013.

(8) Collin Anderson, "Dimming the Internet :Detecting Throttling as a Mechanism of Censorship in Iran", *Iran Threats*. arXiv, 18 June 2013. https://arxiv.org/pdf/1306.4361.pdf

وفي مواجهة هجمات مثل (ستوكسنت)، أدى اضطرار طهران لتقديم وعود بتوفير بدائل محلية إلى تسهيل تنفيذ إجراءات أكثر شمولاً وتحديداً على المستوى الوطني. ومن بين هذه البدائل: الانقطاع التام للاتصالات الدولية، ووضع قدرات المعالجة كأولوية، وإنشاء الصمامات، والتقييد المؤقت لمعدل نقل البيانات. وبما أن البديلين الأخيرين يهددان بإبطاء المكونات الرئيسة للمعاملات والمهام التجارية اليومية؛ فإن هذه الإجراءات لا تزال تعكس مخاوف لدى قطاعات من الإيرانيين فيما يتعلق بمدى استخدام الحكومة لقبضتها على الإنترنت لفرض المزيد من الرقابة.

وفي نهاية المطاف، لا تقلل مركزية إيران في التناظر المحلي -من خلال نقاط تحكم رئيسة- من اعتمادية البنية التحتية للإنترنت بالضرورة، وهي الاعتمادية المهمة جداً لصيانة القدرات، سواء مع التيار الرئيس أو ضده. واتضح هذا جليّاً في أكتوبر ٢٠١٢م عندما زُعم أن حزب العمال الكردستاني قام بتفجير أنابيب توصيل الغاز الطبيعي الإيراني إلى تركيا. ولم يؤثر الدمار المتعلق بالطاقة الحركية على تدفق الغاز فقط، لكنه أيضاً عطّل حركة الاتصال بالإنترنت مع شمال إيران، بالإضافة إلى العراق. وتعود الألياف البصرية التي تم تركيبها إلى جوار أنابيب البترول والغاز إلى شركة خدمات الإنترنت والتليفون المحمول التركية (ترك سيل سوبر أونلاين) التي تعمل مع شركة الاتصالات الإيرانية.

ويبدو أن استراتيجيات إيران في الرقابة اتخذت اتجاهاً تاريخياً لزيادة الإحكام على ضبط عمليات التشويش عند النظر إليها من منظور مستوى الدقة في الترميز الحاسوبي والشبكي؛ فبينما تزامن مع انتخابات يونيو ٢٠٠٩م انقطاع خدمات الرسائل القصيرة على المحمول والذي استمر عدة أسابيع، مع بداية ربيع ٢٠١٣م، أصبحت الفلترة أمراً اعتياديّاً باستخدام كلمات مفتاحية، خصوصاً فيما يتعلق بالمفاهيم السياسية أو الشعارات. وفي فبراير ٢٠١٢م تحول حجب بروتوكول المنافذ الآمنة SSL إلى حجب البروتوكول عن شبكات بعينها فقط، وإعادة توجيه الحركة الآمنة عن طريق اعتراض طلب نظام أسماء النطاقات DNS الذي يساعد على تحديد مكان خدمات وأجهزة الكمبيوتر المتصلة بالإنترنت.

وعلى المنوال ذاته، اعتمد مستخدمو الإنترنت الإيرانيون سُبلاً أكثر احترافيةً؛ لإيقاف الرقابة والتدخل الناشئ من خلال وسطاء محليين. وكانت النتيجة استخدام استراتيجيات

متطورة، منها أدوات منع الفلترة مثل: (تور) و(سايفون)؛ لتمويه حركة المرور على الشبكات، وجعلها أكثر عشوائيةً بطريقة تزيد من كلفة التحقق والفحص التطفلي.

وهناك اتفاق عام على أن إيران تذهب بعيداً لترشيد قدراتها الإلكترونية، ليس فقط على المستوى الاستراتيجي، ولكن أيضاً على مستوى أجهزتها السياسية والأمنية المتداخلة؛ ففي عام ٢٠١٢م أعلن آية الله علي خامنئي المرشد الأعلى للثورة الإسلامية، إنشاء المجلس الأعلى للفضاء الإلكتروني الذي يضم: ممثل خامنئي في المجلس الأعلى للأمن القومي، والمتحدث باسم البرلمان، وقائد قوات الحرس الثوري، ورئيس القضاء الأعلى، وقائد قوات الشرطة، والمسؤولين عن قطاعات البث الرسمي وتكنولوجيا المعلومات والعلوم(٩).

وفي العام ذاته، أعلنت القوات المسلحة الإيرانية تأسيس المقر الإلكتروني الرئيس الذي سيعمل عن كثب مع لجنة المجلس الإلكتروني وعدد من الوحدات مثل: السياسة، والاقتصاد، والشريعة الإسلامية؛ لمواجهة ما تسميه إيران الحرب الناعمة ضدها(١٠). وإضافة إلى هذا، يُقال إن الآلاف من الخبراء التقنيين تلقوا تدريباً من قائد قوات الدفاع الإلكتروني في الحرس الثوري الإيراني؛ للتجسس على المنشقين، ومراقبة الجاليات الإيرانية في بلاد المهجر، ومنها: الولايات المتحدة والسويد وألمانيا.

٣- السعودية في مرمى الهدف: (شامون) و(شامون ٢)

بما أن إيران عززت من قدراتها الإلكترونية ورشَّدتها بعد هجمة ستوكسنت؛ فقد أصبح مشتبهاً بها لشنِّ هجمات ثأرية على المستويين الإقليمي والدولي في عددٍ من الحالات؛ فعلى سبيل المثال، هناك هجمة أغسطس ٢٠١٢م التي استهدفت شبكة الحاسوب في شركة أرامكو السعودية. ولم تؤذِ الهجمة التي أُطلق عليها (شامون)، والتي شنها على الأرجح قراصنة إيرانيون، مكونات الحاسوب الصلبة، ولكنها نجحت في مسح البيانات

(9) Barbara Slavin and Jason Healey. :Iran: How A Third Tier Cyber Power Can Still Threaten the United States", *Atlantic Council Issue Brief*, July 2013, p.4. http://www.atlanticcouncil.org/publications/issue-briefs/iran-how-a-third-tier-cyber-power-can-still-threaten-the-united-states

(10) Joanna Paraszczuk, "Iran Establishes Cyber HQ as Shadow War Continues", *Jerusalem Post*, December 3, 2012. http://www.jpost.com/Iranian-Threat/News/Iran-establishes-cyber-HQ-as-shadow-war-continues

المسجلة على الأقراص الصلبة في نحو ثلاثين ألف جهاز حاسوب. وفي دليل على الافتقار إلى المرونة والخطة البديلة بعد الهجوم، تقول التقارير إن الشركة لجأت إلى ست شركات متخصصة في أمن المعلومات للتحضير لتحقيق جنائي. وكان على (أرامكو) أيضاً إرسال مشترين إلى آسيا لجلب آلاف من الأقراص الصلبة البديلة.

وبينما فشل الهجوم في تعطيل أو عرقلة الإنتاج، فقد سبَّب قطعاً في خسائر مالية لا يمكن تجاهلها، إضافة إلى الضرر المعنوي الذي لا يمكن قياسه. وذهبت التحقيقات إلى أن الهجوم تضمن التصيد الاحتيالي، ورسائل بريد إلكتروني مزيفة تحاول خداع المستخدمين للانخراط في تفاعلات تسمح للمخترقين بتثبيت برمجيات خبيثة على الحاسوب سراً بهدف السيطرة على النظام الإلكتروني. وبهذا؛ دفع (شامون) أرامكو -كبرى الشركات المنتجة للبترول في العالم- إلى عزل أجزاء من نظامها الإلكتروني، وحجبه عن الاستخدام الخارجي. ولم تستطع التحقيقات إثبات أي دليل على تورط أي من موظفي الشركة من الداخل.

وأعلنت مجموعة تطلق على نفسها (سيف العدالة القاطع) مسؤوليتها عن الهجوم الذي كان مرتبطاً بإيران -على عهدة الوول ستريت[11]-، وكانت دوافعها سياسية إلى حدٍ كبير؛ إذ اتهم المخترقون المملكة العربية السعودية بارتكاب مذابح في البحرين وسوريا.

وبعد أسبوعين فقط من حادث (أرامكو)، تعرضت شركة (راس غاز) -ثاني أكبر منتج وناقل للغاز الطبيعي المسال في قطر- إلى هجمة إلكترونية. وأثرت البرمجيات الخبيثة، ابتداءً بشكلٍ كبير، في استخراج الغاز ومعالجته. وفوق ذلك تبيّن الحادثتان التداعيات والتبعات الأبعد عندما يتم استهداف الشركات بهجمات إلكترونية. وتعتمد الاقتصادات الحديثة كثيراً على الإمدادات غير المنقطعة من البترول والغاز بسعرٍ معقول؛ وبالتالي فإن أي انقطاع في هذه الإمدادات من السعودية وقطر سيفاقم الأزمة الاقتصادية العالمية في قطاع الطاقة، وقد ينعكس ذلك على شكل اضطرابات في البورصات العالمية.

وأصدرت السلطات السعودية في نوفمبر ٢٠١٦م تحذيرات تنصح باليقظة والحذر في ضوء ظهور عدة تطورات لدودة شومان. وكررت السلطات هذه التحذيرات مراراً منذ

(11) Siobhan Gorman and Julian E.Barnes, "Iran Blamed for Cyberattacks", *The Wall Street Journal*, October 12,2012. https://www.wsj.com/articles/SB10000872396390444657804578052931555576700

يناير ٢٠١٧م. كما انتشرت إنذارات أخرى متزامنة مع تعرض وزارة العمل السعودية، ومركز الصناعات البتروكيماوية في المنطقة الشرقية، إلى مشكلات مماثلة في شبكاتها الإلكترونية. وأصبحت شركة (صدارة) التي تعمل برأس مال سعودي - أمريكي، الضحية التالية؛ إذ اضطرت إلى غلق شبكتها الحاسوبية، ولكن هذا الإغلاق الاضطراري لم يؤثر في قدراتها التشغيلية داخل مرافقها بمدينة الجبيل الصناعية.

ويقول المعلقون إن تصميم (شامون ٢) يشير إلى طبيعته الاختراقية، وأنه يشبه كثيراً تصاميم سابقة صدرت عام ٢٠١٢م. وحتى الفحص التقني المكثف للهجوم كشف عن متشابهات واضحة في ملفات (الدوس) التي تسببت في مسح البيانات بالنظم المصابة[١٢]. وعلى مستوياتٍ مختلفة، يعد هذا مفاجأة؛ إذ عادةً ما يُتوقع من المهاجمين أن يخفوا استراتيجياتهم للاختراق بإضافة متغيرات وتحديثات؛ تماشيّاً مع مبدأ التكيف، وتجهيزاً لإجراءات وقائية مضادة أكثر جرأةً من تلك التي واجهوها سابقاً.

يقول ديميتري ألبيروفيتش المدير التنفيذي للتقنية في شركة الأمن الرقمي (كراودستريك)، إن إحدى أهم سمات (شامون ٢) هي وضع صورة جثة الطفل السوري ذي السنوات الثلاث الذي جرفته الأمواج إلى أحد شواطئ تركيا عام ٢٠١٥م على شاشة سطح المكتب للأجهزة المصابة. وفي عام ٢٠١٢م، ترك (شامون) صورة علم أمريكي يحترق قبل تعطيل النظم الإلكترونية المستهدفة[١٣]. ولا يمكن غض النظر عن هذه الرمزية التي تلقي الضوء على التوتر القائم بين الدول على ضفتي الخليج العربي [يستخدم النص الإنجليزي لفظ (الخليج الفارسي)] في الإطار الجغرافي - السياسي والاستراتيجي الأوسع في المنطقة. وتزداد أهمية إظهار القدرات الإلكترونية الهجومية -بوصفها عملاً يعكس المصالح القومية الصامدة- من خلال استخدام وسائل حرب تطفلية في المجال الإلكتروني. ومن منظور دفاعي وهجومي تتماشى هذه القراءة مع تزايد أهمية المجال الإلكتروني في الأمن القومي[١٤]. وبالمثل، تتزايد أهمية تقوية التنسيق الإقليمي لقطع الطريق أمام

(12) *Vectra Networks*, Blogpost by Greg Linares, "An analysis of the Shamoon2 malware attack", February 7, 2017. https://blog.vectranetworks.com/blog/an-analysis-of-the-shamoon-2-malware-attack

(13) Dmitri Alperovitch, "Shamoon Round 2 or the Power of Machine Learning", December 1, 2016, https://www.crowdstrike.com/blog/shamoon2/

(14) Timothy Edmunds, "Complexity, Strategy and the National Interest", *International Affairs* 90:3, 2014. 533-534.

التهديدات الإلكترونية التي تستهدف دول مجلس التعاون الخليجي؛ وهو ما انعكس على كلمة صالح المطيري مدير عام المركز الوطني للأمن الإلكتروني في وزارة الداخلية، خلال المؤتمر الدولي الثاني للأمن الإلكتروني الذي عُقد في الرياض أواخر فبراير ٢٠١٧م[١٥].

٤- إرباك الغرب: عمليتا زهرة الزعفران وأبابيل

في عام ٢٠١٣م، وبعد ثلاثة أعوام من اكتشاف دودة ستوكسنت، أصدرت شركة الأمان الإلكتروني (فايرآي)، ومقرها كاليفورنيا بالولايات المتحدة، تقريراً مُفصّلاً عن تزايد أنشطة تهديدات ما يُطلق عليه (فريق أمان أياكس) الإيراني، وربطته الشركة بإيران من خلال الكشف عن تزايد الهجمات التي أُطلق عليها اسم زهرة الزعفران، والتي تستهدف شركات الدفاع الأمريكية والمعارضة الإيرانية في الخارج. ويؤكد نارت فيلينوف، وهو باحث مختص في التهديدات الاستراتيجية بشركة فايرآي، أن هذه الجهود تتسق مع محاولات إيران للسيطرة على المعارضين السياسيين عن طريق التوسع في قدراتها الإلكترونية، ويدّعي أن "إيران لا تتوسع فقط في قدراتها الإلكترونية، بل إنها انتقلت إلى مرحلة استخدام تقنيات تجسُّس إلكترونية متقدمة؛ إذ لا تقتصر الهجمات فقط على نشر الرسائل، بل للتسلل واختراق النظم وتقويضها على المدى الطويل".

ويضيف فيلينوف: "تنخرط المجموعة التي تمتد جذورها إلى منتديات المخترقين الإيرانيين مثل إيشيان وشابجارد، في هجمات على مواقع إلكترونية منذ ٢٠١٠م. ولكن بحلول عام ٢٠١٤م، كانت المجموعة قد تحولت إلى مجموعة تجسُّس متخصصة بالبرمجيات الخبيثة، وباستخدام منهجية تتماشى مع تهديدات أخرى متطورة ومستمرة في المنطقة"[١٦].

واستهدف فريق أمان أياكس أيضاً مستخدمين إيرانيين محليين يستخدمون تقنيات معادية للرقابة مثل (بروكسي فاير)، و(بروسيفين)؛ حيث إنهما يستطيعان تجاوز

(15) IISS Cyber Report: 23 February to 2 March 2017. http://www.iiss.org/en/iiss%20voices/blogsections/iiss-voices-2017-adeb/march-8a0c/cyber-report-23-february-to-2-march-0217

(16) Pierluigi Paganini, "Ajax Security Team lead Iran-based hacking groups", *Security Affairs*, May 13, 2014. http://securityaffairs.co/wordpress/24923/cyber-crime/ajax-security-team-iran.html

نظام الرقابة الإلكتروني الإيراني. وبينما لا يزال من غير الواضح إذا ما كان فريق أياكس يعمل منفرداً أو كجزء من فريق أكبر ربما تابع للدولة، فإنه يمكن القول إنه يستخدم أدوات خبيثة لا تتوافر للأفراد؛ فهو يستخدم الكثير من تقنيات الهندسة التناسلية لإغراء المستهدفين، والتأثير فيهم، وضرب أنظمتهم ببرمجيات خبيثة مصمَّمة خصيصاً لهذا الغرض. وربما يمتلك الفريق أيضاً أدوات وشفرات تُمكنه من إطلاق هجمات مكثفة على مدار أيام متوالية.

وكشفت شركة فايرآي كذلك معلومات عن نحو ٧٠ وجهة مشتبهاً بها بثّت رسائل من خادم واحد للقيادة والسيطرة. واكتشفت الروابط عندما وجدت عينات تحليل البرمجيات الخبيثة علامات تشير إلى أنها كانت مخفية وغير مرئية لوسائط لنظم إيرانية وظيفتها كسر الرقابة. وكشف الفحص نمطاً مشتبهاً به؛ إذ ضُبطت معظم الأهداف على توقيت إيران، واستُخدمت فيها اللغة الفارسية. وإضافة إلى ذلك، استخدم ثلث عدد الأجهزة التي لم تضبط على التوقيت الإيراني -عن عمد- اللغة الفارسية، بينما استخدم الثلثان الباقيان نظامي بروكسي فاير وبروسيفين.

يعد هذا مثالاً واضحاً ودقيقاً، لكنه جاء مشابهاً لأمثلة أخرى عديدة؛ فقد ارتبطت إيران بالهجمات الإلكترونية المتقدمة منذ ٢٠٠٩م، عندما كشفت مروحية تابعة لمشاة البحرية الأمريكية فجأة شبكة مشاركة ملفات إيرانية[١٧]. وبعدها بعام، أوقف ما يُطلق عليه (جيش إيران الإلكتروني) محرك البحث الصيني بايدو، في ردٍّ على المنصة التي تتحدث سلباً عن الرسائل السياسية المنبثقة عن إيران.

وفي عام ٢٠١٣م، ذكرت صحيفة وول ستريت أن الفاعلين الإيرانيين كثفوا جهودهم التي تعمل على عرقلة مرافق البنية التحتية الأمريكية المهمة. وخلال السنوات الأخيرة، أطلقت مجموعة أخرى تسمي نفسها (القسام) عملية (أبابيل) التي تسبَّبت في سلسلة من هجمات حجب الخدمة استهدفت المؤسسات المالية الأمريكية الكبرى، ومنها بورصة نيويورك. وبالتزامن مع هذا، أغرقت القسام المواقع الإلكترونية للبنوك بطلبات التشفير. وبما أن هذه العمليات تتلف موارد كبيرة للنظم الحاسوبية، ومنها -على سبيل المثال-

(17) Martti Lehto and Pekka Neittaanmäki (Eds.), *Cyber Security: Analytics, Technology and Automation* (Springer International Publishing: Switzerland), 2015, 74.

ما يحدث عند التعامل مع عمليات العملاء المشفرة عبر الإنترنت؛ فإنه من الممكن أن تعاني البنوك من عطل مؤقت في الخادم أو حتى تلفه تماماً. وضربت هذه العمليات مؤسسات كبرى مثل: ويلز فيرجو، ويو أس بانكروب، وأتش أس بي سي، وجي بي مورغان تشاس، وسيتي جروب.

وفي الوقت ذاته من أبريل ومايو ٢٠١٣م، شعر المسؤولون الأمريكيون وخبراء أمن تكنولوجيا المعلومات بالقلق إزاء سلسلة من الهجمات الإلكترونية المدمرة التي ضربت شركات أمريكية للطاقة، والتي تم شنّها غالباً بهدف استكشاف طرق ممكنة للسيطرة على نظم المعالجة، مثل أنابيب البترول؛ تمهيداً لهجمات مستقبلية. وبعد بحث مضنٍ استغرق شهراً، تم تحديد إيران كمصدر محتمل للهجوم؛ مما عجّل بصدور تحذير أطلقته وزارة الداخلية. وكان هذا الهجوم متعدد المحاور الذي أصاب قطاع الطاقة في الولايات المتحدة، متطوراً ومعقداً بما يسمح بتبنّي القول بقيام السلطات الإيرانية بإصدار الأمر بشنّ هذا الهجوم، على الرغم من عدم وجود دلائل قطعية بهذا[١٨].

وفي الصورة الكاملة، تلقي هذه الاعتداءات الضوء على إصرار إيران، وعلى التقدم الذي حققته في تطوير قدراتها الاختراقية والهجومية. وعلى الرغم من أن منطق الهجوم على قطاعي الطاقة والمال في الولايات المتحدة يشابه نمط الهجوم على أرامكو السعودية وراس غاز القطرية في العام السابق، إلا أنه من الصعوبة بمكان، إن لم يكن مستحيلاً، عزو الهجمات الإلكترونية السياسية إلى مَن قام بها إذا ما نُفذت بحرفية. وحتى إذا ما كان يمكن تتبع الهجوم والوصول إلى دولة معينة، وحتى إذا ما كانت دوافعها واضحة، تبقى العوامل التقنية والاجتماعية والسياسية عائقاً بحيث تعطى الدولة المتهمة مساحة واسعة للإنكار[١٩].

ربما تشير القدرات والتطورات اللازمة لتصميم هجمة إلكترونية وإطلاقها إلى أن هذه الجهود غير مدفوعة بأسباب مرتبطة بجرائم إلكترونية تقليدية في الحالات التي لم يتم فيها اختراق حسابات بنكية أو الاستيلاء على أصول للعملاء مثلاً. ولكن هذه المناطق

(18) Nicole Perlroth and David E.Sanger, "New Computer Attacks Traced to Iran, Officials Say", *The New York Times*, May 24, 2013. http://www.nytimes.com/2013/05/25/world/middleeast/new-computer-attacks-come-from-iran-officials-say.html

(19) Thomas Rid, "Cyber War Will Not Take Place» (London: C Hurst & Co Publishers Ltd), 2013.

الرمادية التي تجعل الإسناد النهائي صعباً هي جزء من الاستراتيجية التي ربما تشير إلى الانخراط العسكري تحت حماية الحكومة الإيرانية؛ للانتقام من الهجمات الإلكترونية الغربية ونظام المقاطعة الاقتصادية. أو بكلمات مايكل هايدن الرئيس السابق لوكالة الاستخبارات ووكالة الأمن القومي الأمريكية: "لقد أصبحت أخشى دولة لن تواجهنا وجهاً لوجه في معركة تقليدية بعد أن اكتشفت فجأة الآن أنها يمكن أن تأسر انتباهنا بالهجمات الإلكترونية"[٢٠].

٥- الأنشطة بالوكالة في سوريا واليمن ولبنان

في إبريل ٢٠١٣م، نجح ما يُطلق عليه (الجيش السوري الإلكتروني)، وهو مجموعة من المهاجمين الذين يدعمون نظام بشار الأسد ويرتبطون بإيران غالباً، في اختراق الحساب الإلكتروني لوكالة الأسوشيتد برس، وأرسلوا تغريدة مزيفة تدَّعي تفجير البيت الأبيض؛ ما أدى إلى خسائر بلغت ١٣٠ مليار دولار أمريكي بحساب السوق[٢١]، وتراجع في بورصة نيويورك.

وأطلقت المجموعة أيضاً هجمات إلكترونية مدمرة استهدفت المعارضة السورية منذ اندلاع الثورة في ٢٠١١م [يستخدم النص الإنجليزي لفظ الحرب الأهلية]، وغالباً ما تستخدم أسماء مستعارة لتحقيق غاياتها. ويشير استخدام الجيش السوري الإلكتروني الكثيف للفضاء الإلكتروني بحرفية إلى تورط مستشارين إيرانيين في تدريب عناصر من الجيش السوري، بالتزامن مع الوجود الفعلي للاستخبارات الإيرانية التي تشرف على العملية العسكرية لقوات الأسد في سوريا. وضربت هجمات التجسُّس التي شنها الجيش الإلكتروني السوري في نهاية ٢٠١٣م عدداً من الشخصيات رفيعة المستوى في المعارضة السورية مثل اللواء سليم إدريس رئيس هيئة الأركان بالمجلس العسكري الأعلى للجيش الحر سابقاً.

---

(20) Reuters Summit News, Cyber experts warn Iranian hackers becoming more aggressive, May 13, 2014. http://www.reuters.com/article/us-cyber-summit-iran-hackers-idUSBREA4C03O20140513

(21) Max Fisher, The Washington Post, Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?, April 23,2013. https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/?utm_term=.cae0913d3cae

وفي ربيع وصيف ٢٠١٥م ظهرت مجموعة باسم جيش اليمن الإلكتروني، وادَّعت أنها اخترقت أنظمة الحكومة السعودية، ومنها وزارات: الداخلية والدفاع والخارجية. وطبقاً لتصريح لجريدة الحياة اللندنية (المملوكة للسعودية) كانت البنية التحتية الإلكترونية أيضاً عرضةً لمحاولات من قبل جيش اليمن الإلكتروني الداعم للحوثيين؛ إذ ظهرت شعارات مناهضة للغرب وللسعودية باللغة العربية؛ مما يطرح فرضية تورط إيران.

ومن الملاحظ أن هجمات جيش اليمن الإلكتروني تعرض في بعض الأحيان شعار (جيش العدالة القاطع)، وهو الشعار ذاته المستخدم في الهجمة على شركة أرامكو عام ٢٠١٢م، ونادراً ما كان هذا الشعار يظهر على مواقع إنترنت أخرى. وإضافة إلى ذلك، كانت أخبار أنشطة جيش اليمن الإلكتروني ترد حصرياً على الصفحات الأولى في صحيفتي فارس نيوز، ونيوز كويك ليك الإيرانيتين؛ ما يثبت تورط إيران في تلك الأنشطة. ومثله مثل لواء القسام والجيش الإيراني الإلكتروني، يتجنب جيش اليمن الإلكتروني غالباً الظهور العلني ولفت الأنظار في أنشطته الدعائية على وسائل التواصل الاجتماعي، وهي سمة غريبة نوعاً ما إذا ما وضعنا في الحسبان أنه يعمل بشكل مستقل دون توجيه استراتيجي شامل.

وبالنظر إلى لبنان البلد الذي عانى من الانقسامات السياسية الممتدة على مدى أكثر من جيل، لا نستغرب أن حليف إيران الرئيس (حزب الله) انخرط هو أيضاً في أنشطة القرصنة الإلكترونية. ويسلط تقرير صدر في مارس ٢٠١٣م عن تشيك بوينت؛ وهو مزوّد إسرائيلي لأمن تكنولوجيا المعلومات، الضوء على مخططات وطبيعة عمليات الهجوم الإلكتروني الذي أطلق عليه (الأرز المتطاير)؛ ما يشير إلى دلائل أثارت الشكوك حول أن مصدر هذا التهديد كان من لبنان، وربما بدعم من إيران[٢٢]. وقد استهدفت تلك البرامج الخبيثة شركات متعددة الجنسية وقطاعات للدفاع في كل أنحاء العالم منذ عام ٢٠١٢م.

٦- ربط النقاط: يد إيران الإلكترونية الطولى حول العالم

في صيف ٢٠١٥م، أصدر كليرسكاي، وهو خادم استخباراتي إلكتروني، تقريراً

(22) CheckPoint Software Technologies Ltd., Volatile Cedar, Threat Intelligence and Research Report, March 30, 2015. https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf

مفصلاً عن استخدام أشد تدميراً للبرمجيات الخبيثة، وهو شفرة باسم (غولي)؛ ففي أكثر من ٥٠٠ حالة، اخترق (غولي) الأهداف، نصفها تقريباً في السعودية، و١٤ في المئة منها في إسرائيل. وتضمنت سمات هذا البرنامج الخبيث استخدام اللغة الفارسية، وتغيير لغة الصفحات إلى الفارسية. وبعد تتبع تلك العناوين وجد أنها تعود إلى مواقع في إيران[٢٣].

وليس من قبيل المصادفة أن سمات (غولي) التي اكتشفها كليرسكاي هي ذاتها التي اكتشفتها فايرآي في فريق أياكس للأمان. وتتسق التحقيقات الجنائية الخاصة بالخروقات الإلكترونية في مناطق أخرى من الشرق الأوسط وأوروبا مع سرديات الفاعلين داخل إيران.

وفي مارس ٢٠١٥م كشفت شركة الأمن اليابانية (ترينديمايكرو) هجمات إلكترونية مشابهة لغولي في ألمانيا وإسرائيل أطلقت عليها (السمكة الذهبية) يُفترض أنها دُشّنت على يد مجموعة مخترقين تدعمهم الحكومة الإيرانية. ويُوصف الهجوم بأنه سهل تقنيّاً إلى حدٍ ما، ولكنه يعد مناورة مؤثرة جداً للتجسس وتصيُّد البيانات. وكجزء من التحقيق، عُزي الهجوم إلى مجموعة المخترقين الإيرانية (روكست كيتن)؛ حيث يُفترض أن مهدي مهدافي طوّر الهجوم من برنامج حميد كان متوفراً عام ٢٠١١م.

واعتمد هجوم السمكة الذهبية على رسائل بريد إلكتروني تصيُّدية يُفترض أنها موجهة إلى أشخاص رفيعي المستوى. وتحتوي الرسالة على رابط يوجِّه الضحية إلى ملف على خادم تخزين مجاني على الإنترنت يصيب النظام الإلكتروني المستهدف. وكل التفاصيل التقنية وتسلسلها موجودة على الموقع الإلكتروني لترينديمايكرو.

وكما ذُكر سابقاً، فمنهجية الهجوم ذاتها ليست جديدة، ولا استثنائية، ولا معقدة. ولكن هذا لا يبخس نجاحها الذي يتضح من العدد الكبير للضحايا المستهدفين. وإلى جانب إيران، تمارس الصين وروسيا أيضاً هجمات التصيُّد الاحتيالي؛ إذ تمتلكان كلَّ خصائص التهديد المتقدم المتكرر.

---

(23) ClearSky Cyber Security, Thamar Reservoir – An Iranian cyber attack campaign against targets in the Middle East, June 3, 2015. http://www.clearskysec.com/thamar-reservoir/

وفي حالة (السمكة الذهبية) -كما في حالات مماثلة- كان البرنامج الخبيث يختبئ في رسالة إلكترونية بسيطة. وتتكيف هذه الرسائل مع المعايير الرسمية التي يعتاد عليها أي مرسل إليه؛ فلا يكون لديه أي سبب واضح للشك والامتناع عن الضغط على الرابط أو الملحق. وعادةً ما يسبق هذه الهجمات مقاربات منهجية متقدمة يُطلق عليها الهندسة الاجتماعية، وتشير إلى المناورات الشخصية لحث سلوك ما بعينه، مثل محاولة الدفع إلى إفشاء معلومات سرية أو شراء منتج أو الإسهام المالي. ويتسلل (المهندسون الاجتماعيون) داخل المحيط الشخصي للضحايا، ويزيفون الهويات أو يدّعون أنهم مخوّلون –مثلاً– بالحصول على معلومات سرية أو تقديم خدمات من دون مقابل.

وفي نوفمبر ٢٠١٤م، كشفت وكالة الاستخبارات الداخلية لولاية بافاريا الألمانية أن هجمات إلكترونية إيرانية استهدفت عدة مراكز أبحاث ألمانية وشركات متعددة الجنسية في بلاد أوروبية أخرى إلى جانب الولايات المتحدة وإسرائيل والمكسيك والصين. ويدَّعي هذا التقرير سرقة كميات ضخمة من البيانات، ومنها مواد حساسة متعلقة بالصناعات التكنولوجية العسكرية والمدنية مثل الصواريخ والمروحيات والأقمار الصناعية. ووجد المحققون خادماً حفظ عليه المهاجمون المزعومون الملفات المسلوبة من الضحايا، إضافة إلى الأدوات المستخدمة؛ مما أدى إلى كشف ساعات عمل المهاجمين وعناوين مواقعهم على الإنترنت؛ وهو ما يشير إلى إيران في نهاية المطاف.

وقد صُممت القدرات الإلكترونية الحالية للحكومة الألمانية لحماية المؤسسات والتجارة من الأنشطة الاحتيالية والتجسُّس، ولكنها -بوضعها الحالي- لا توازي طموح قطاع الأمن أو القدرة على تحديد مصدر التهديد، ناهيك عن العمل على وسائل مناسبة لإطلاق هجوم مضاد. المحصلة النهائية أن تحديد المصدر -على الأقل من المنظور الأوروبي- يعمل على المستوى السياسي مثلما يعمل على القدرات التقنية والبنية التحتية.

الخاتمة

على النقيض؛ فإن تصنيف الخط العمودي الذي تم تقديمه في الحالات المتعددة السابقة يتوافق ويصطف مع المناخ الجيوسياسي الذي تحكمه مصالح الدول، ويشير إلى دوافع تحقيق الأهداف من خلال التجسُّس والتخريب الرقمي، فضلاً عن تحقيق المكاسب المالية عن طريق نشاطات القرصنة. وبالتالي؛ فمن المتوقع أن يحمل لصعود إيران وإصرارها السياسي منفذاً رقمياً كامتداد لحملات الوكالة التي تشنها عبر المنطقة؛ لذلك فمن المنطقي أن نربط بين صعود إيران السياسي وإصرارها على مواصلة هجماتها الإلكترونية على نحو متزايد، وأنه امتداد لحملاتها الجارية في كل أنحاء المنطقة.

وهناك أيضاً عامل أبعد؛ فقد خلصنا إلى أن أنشطة إيران الإلكترونية مصمَّمة وموجهة لتحقيق أهدافها الجيوسياسية، ليس فقط في المنطقة، ولكن لمواجهة الدفاعات الإلكترونية لإسرائيل والدول العربية الصديقة، وكذلك دفاعات الولايات المتحدة. وبعيداً عن المشكلات التي تسبَّب فيها فيروس ستوكسنت، فإن هجمات القرصنة العدوانية تلك لم تكلّف إيران سوى القليل جداً. وكما أوضحت الصين وروسيا، فإنه يمكن إلحاق الكثير من الفوضى والاضطراب بالعدو من خلال الهجوم الإلكتروني، وبمخاطر محدودة للغاية.

هناك احتمالية ضعيفة للغاية بأن يقوم المجتمع الدولي في المستقبل -من خلال مجلس الأمن مثلاً- بالتأسيس لمقاربة تحدُّ من مخاطر الدول (العدوانية إلكترونياً) مثل إيران. وعلى هذا النحو، سيكون على مَن يواجهون إيران في الشرق الأوسط، وما وراءه بشكلٍ شبه مؤكد، أن يواجهوا نظاماً دينياً قائماً على إزعاج النظام الدولي.

نبذة عن الكاتبين

جاك كارافيللي

لدى الدكتور كارافيللي مسيرة مهنية حافلة في الخدمة المدنية تتضمَّن مناصب تحليلية وقيادية في وكالة الاستخبارات المركزية، ومجلس الأمن القومي التابع للبيت الأبيض؛ حيث كان من كبار مستشاري الرئيس بيل كلينتون فيما يتعلق بملف روسيا والشرق الأوسط وملفات قضايا منع الانتشار النووي، ووزارة الطاقة؛ إذ ترأس برامج تقليل المخاطر النووية الدولية. وبعد تركه العمل الحكومي، ألّف كارافيللي أربعة كتب، وتناول الكثير من قضايا الأمن القومي في الولايات المتحدة وخارجها. وفي عام ٢٠١٥م ترأس مؤتمراً دوليّاً في سويسرا حول الأمن الإلكتروني، وسيترأس مؤتمراً دولياً آخر في أكسفورد لاحقاً هذا العام. وهو يكتب بانتظام عن القضايا الإلكترونية، ويتحدث في القنوات التلفزيونية والإذاعية. وفي عام ٢٠١٦م، ترأس كارافيللي شركة نيوجين، وهي شركة استشارات تكنولوجية عالمية.

سبستيان ماير

التحق ماير بمركز الملك فيصل للبحوث والدراسات الإسلامية عام ٢٠١٥م كباحث مقيم. وينصبُّ اهتمامه على الاتجاهات السياسية – العسكرية في الشرق الأوسط، والأزمة السورية، وتورُّط روسيا وإيران وحزب الله في الشام. وسبق أن عمل متدرباً في السفارة الكندية بألمانيا، كما عمل بمكتب الاتصال السعودي – الألماني للشؤون الاقتصادية في الرياض. وهو حاصل على بكالوريوس العلوم السياسية والقانون عام ٢٠١٣م من جامعة ميونخ الألمانية، ومعهد الدراسات السياسية في باريس، كما أنه حاصل على الماجستير في العلوم الاستخباراتية والأمن الدولي من قسم علوم الحرب في جامعة كينجز كوليدج بلندن. ويعمل في مجال الاستشارات الاستراتيجية للحكومات والشركات منذ عام ٢٠١٦م.

مركز الملك فيصل للبحوث والدراسات الإسلامية

تأسّس المركز سنة ١٤٠٣هـ/ ١٩٨٣م لمواصلة الرسالة النبيلة للملك فيصل بن عبدالعزيز -رحمه الله- في نشر العلم والمعرفة بين المملكة وبقية دول العالم. ويعدُّ المركز منصةَ بحثٍ تجمع بين الباحثين والمؤسسات لحفظ العمل العلمي ونشره وإنتاجه، وإثراء الحياة الثقافية والفكرية في المملكة العربية السعودية، والعمل بوابةً وجسراً للتواصل شرقاً وغرباً. ويرأس مجلس إدارة المركز صاحب السمو الملكي الأمير تركي الفيصل بن عبدالعزيز، وأمينه العام هو الدكتور سعود بن صالح السرحان.

ويقدّم المركز تحليلات متعمّقة حول القضايا السياسية المعاصرة، والدراسات السعودية، ودراسات شمال إفريقيا والمغرب العربي، والدراسات الإيرانية والآسيوية، ودراسات الطاقة، ودراسات اللغة العربية والحداثة. ويتعاون المركز مع مؤسسات البحث العلمي المرموقة في مختلف دول العالم، ويضمّ نخبةً من الباحثين المتميّزين، وله علاقة واسعة مع عددٍ من الباحثين المتخصّصين في مختلف المجالات البحثية. ويحتضن المركز مكتبة الملك فيصل، ومجموعة مخطوطات نادرة، ومتحفاً إسلامياً، وقاعة الملك فيصل التذكارية، وبرنامج الباحثين الزائرين. ويهدف المركز إلى توسيع نطاق المؤلَّفات والبحوث الحالية لتقديمها إلى صدارة المناقشات والاهتمامات العلمية، متّبعاً مساهمة المجتمعات الإسلامية في العلوم الإنسانية والاجتماعية والفنون والآداب قديماً وحديثاً.

مركز الملك فيصل للبحوث والدراسات الإسلامية
King Faisal Center for Research and Islamic Studies

P.O.Box 51049 Riyadh 11543 **Kingdom of Saudi Arabia**
Tel: (+966 11) 4652255 Ext: 8692 Fax: (+966 11) 4577611
E-mail: research@kfcris.com