رصد مراكز الدراسات والمواقع التحليلية للنخب العالمية البارزة

العنوان

الصفحه	
٣	الملخص التنفيذي
٤	١. يبدو أن القراصنة الداعمين لإيران قد زادوا من الهجمات السيبرانية ضد البنية التحتية الحيوية / Defense One
٥	٢. تزعم إيران أن الولايات المتحدة عطّلت شبكات الاتصالات أثناء الحرب باستخدام تكتيك الأبواب الخلفية / The Register
٦	٣. تحذر شركة Resecurity من أن الحرب الإيرانية دخلت مرحلة متعددة المجالات، حيث أصبحت العمليات السيبرانية والعسكرية مترابطة ومتشابكة / Industrial
٧	٤. داخل الحرب النفسية التي تشنها إيران ضد خصومها / CNN
٨	٥. على الرغم من وقف إطلاق النار، لم يتوقف القراصنة الإيرانيون عن نشاطهم / The New York Times
٩	٦. كيف يشكّل القراصنة الإيرانيون تهديداً للبنية التحتية الحيوية في الولايات المتحدة / The Conversation
١٠	٧. تصاعد التوتر مع إيران يفاقم التهديدات السيبرانية ضد البنية التحتية للطاقة في الولايات المتحدة / CSIS
١١	٨ تحذيرات عالمية من الحرب السيبرانية الإيرانية وتهديدها للبنية التحتية الحيوية في الولايات المتحدة / القيادة السيبرانية الأمريكية
١٢	٩. الصراع بين إيران وإسرائيل ودور الهجمات السيبرانية البارز والتقنيات الرقمية في مجريات المواجهة / AP News
١٣	١٠. هددت إيران شركات التكنولوجيا الكبرى مثل إنفيديا وآبل وغيرها من عمالقة التكنولوجيا بشنّ هجمات / CNBC
١٤	١١. اختراق المستشفيات، وبرمجيات التجسس الخفية؛ الحرب الإيرانية تُظهر كيف تم دمج القتال الرقمي في الحرب الحديثة / Axios
١٥	١٢. كيف تعيد حرب الشرق الأوسط تشكيل المشهد العالمي للأمن السيبراني / المنتدى الاقتصادي العالمي (World Economic Forum)
١٧	١٣. ارتفاع الهجمات السيبرانية في الإمارات إلى ٥٣٠ ألف حالة يومياً بالتزامن مع الحرب الإيرانية / Wired
١٩	١٤. إيران تستعرض قدراتها السيبرانية / Foreign Policy
٢٠	ملخص وتحليل الخبير

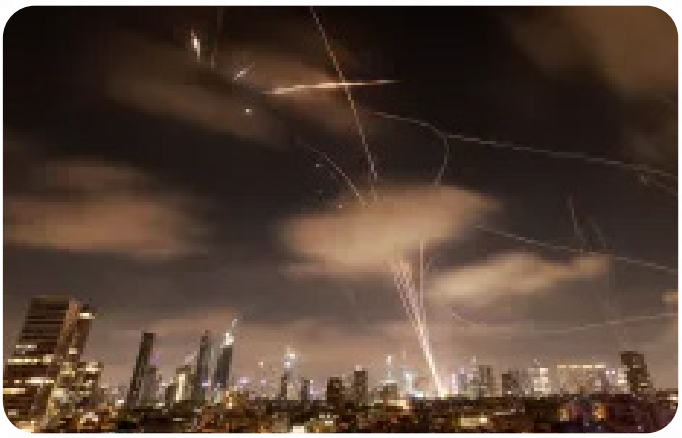
الملخص التنفيذي

تجمع هذه المجلة مجموعة من التقارير والتحليلات حول الحرب الإيرانية وتداعياتها السيبرانية، ويظهر في جميعها رسالة مشتركة: الحرب الإيرانية لا تحدث فقط في الميدان العسكري، بل تجري في الوقت نفسه في الفضاء السيبراني والمعلوماتي والنفسي والاقتصادي. تتمثل الرواية العامة لهذه المجلة في أن القراصنة المرتبطين بإيران، والجماعات الوكيلة، وحتى بعض الفاعلين المتوافقين مع هذا السياق، يستخدمون الهجمات السيبرانية لفرض الضغط، وإحداث الاضطراب، وجمع المعلومات، ورفع التكاليف السياسية والأمنية على الخصوم. هذه الهجمات تكون أحياناً عالية الضجيج، لكنها في الغالب لا تهدف إلى التدمير الفوري، بل إلى التغلغل الخفي، والتهيئة للأزمات المستقبلية، وخلق الخوف وانعدام الثقة. في هذه المجموعة من التقارير، يظهر أهم نمط متكرر وهو استهداف البنية التحتية الحيوية. فقد تم استهداف المياه والطاقة والنقل والمستشفيات ومراكز البيانات وشركات التكنولوجيا وحتى الأنظمة الصناعية مثل وحدات التحكم المنطقي القابلة للبرمجة (PLC) مراراً. وتشير رواية هذا العدد من المجلة إلى أن هذه البنى التحتية شديدة الهشاشة بسبب اتصالها الواسع بالإنترنت، وتقادم المعدات، وتعقيد سلاسل الإمداد، والاعتماد على الشركات الخاصة. وفي هذا السياق، فإن الهجوم على شركة Stryker والتحذيرات الأمريكية الرسمية بشأن أنظمة PLC يوضحان أن التهديد ليس نظرياً، بل يمكن أن يؤدي إلى تعطيل العمليات، وخسائر مالية، وحتى توقف بعض الخدمات الحيوية. ومن أبرز محاور المجلة أن الهجوم السيبراني والحرب الميدانية ليسا منفصلين. ففي تقارير مختلفة، يُشار إلى الرسائل النصية المصابة، وبرمجيات التجسس المثبتة على الهواتف المحمولة، وهجمات حجب الخدمة (DDoS)، والتسلل إلى الكاميرات، وسرقة رسائل البريد الإلكتروني والوثائق الشخصية كأدوات تُستخدم بالتزامن مع الهجمات الصاروخية أو بالطائرات المسيّرة. ووفقاً لرواية هذه المجلة، تحاول إيران والجماعات المرتبطة بها من خلال الجمع بين العمليات العسكرية والرقمية ضرب الأهداف العسكرية من جهة، وإرباك الرأي العام وإثارة الخوف والغموض والإرهاق من جهة أخرى. وهذا ما يجعل الحرب السيبرانية ليست مجرد قضية تقنية، بل جزءاً من الاستراتيجية العامة للحرب. كما تؤكد المجلة أن حرب الروايات في الفضاء السيبراني لا تقل أهمية عن الهجمات نفسها. ففي بعض التقارير، أدت ادعاءات إيران بشأن استخدام الولايات المتحدة لأبواب خلفية (backdoors) أو مهاجمة معدات الشبكات إلى تفاعلات من وسائل إعلام صينية وفاعلين آخرين، مما زاد من تعقيد عملية التحقق. والنتيجة هي تداخل الحقيقة التقنية مع الدعاية السياسية والحرب النفسية، مما يجعل التمييز بين الواقع والرواية أكثر صعوبة. وعملياً، يتم استخدام هذا الغموض كسلاح بحد ذاته. أما البعد المهم الآخر في هذا العمل فهو دور الذكاء الاصطناعي وأتمتة الهجمات. إذ تشير التقارير إلى أن الذكاء الاصطناعي يساهم في زيادة سرعة الهجمات ونطاقها وتعقيدها؛ من التصيّد الإلكتروني (phishing) والاختراق الأولي إلى التحرك داخل الشبكات وإنتاج محتوى مزيف. وقد أدى هذا التحول إلى نقل التهديد من هجمات متفرقة إلى عمليات منسقة ومستمرة.

Defense One

يبدو أن القراصنة الداعمين لإيران قد زادوا من الهجمات السيبرانية ضد البنية التحتية الحيوية

في ١٧ أبريل ٢٠٢٦، نُشر مقال بعنوان الفارسي «يبدو أن القراصنة الداعمين لإيران قد زادوا من الهجمات السيبرانية ضد البنية التحتية الحيوية» بقلم كريس تيل (Chris Teale) في مجلة Route Fifty. تركز الرواية الرئيسية للكاتب في هذا المقال على تصاعد التهديدات السيبرانية ضد البنية التحتية الحيوية في الولايات المتحدة، وتسعى إلى إظهار أن بيئة الأمن السيبراني الأمريكي تدخل مرحلة أكثر توتراً وتعقيداً. يرى الكاتب أنه في الأشهر الأخيرة، وخاصة في



أعقاب تصاعد التوترات السياسية والأمنية بين إيران والولايات المتحدة، ازدادت أنشطة الجماعات القرصانية المتوافقة مع إيران. وفي هذا السياق، يشير إلى مجموعة تُدعى «Ababil of Minab» زعمت أنها اخترقت في مارس ٢٠٢٦ الشبكات الداخلية لهيئة النقل العام في لوس أنجلوس (LA Metro). وقد أعلنت هذه المجموعة عبر رسائل على تطبيق تلغرام أنها تمكنت من الوصول إلى الأنظمة الداخلية لهذه الجهة، رغم أن المسؤولين الرسميين أكدوا أن خدمات النقل العام، بما في ذلك المترو والحافلات، لم تتعرض لأي تعطيل، وأنه تم فقط تقييد الوصول إلى بعض أجزاء الشبكة لأسباب أمنية. ويواصل الكاتب سرده بالإشارة إلى أن صحة هذه الادعاءات لم يتم التحقق منها بشكل مستقل حتى الآن، وأن خبراء الأمن السيبراني يشككون في القدرات الحقيقية لهذه المجموعة. ويؤكد بعض المحللين الأمنيين، مثل تيم ميلر من شركة Dataminr، أن هذه المجموعة لا تمتلك سجلاً واضحاً وموثوقاً في تقارير التهديدات السيبرانية، وبالتالي لا يمكن الحكم بشكل قاطع على قدراتها التشغيلية. ومع ذلك، يشير المقال إلى أنه حتى لو كانت هذه الادعاءات مبالغاً فيها، فإنها تندرج ضمن النمط المعروف لنشاط الجماعات المتوافقة مع إيران. وفي الجزء التالي، يؤكد المقال أن التهديد السيبراني للبنية التحتية الحيوية في الولايات المتحدة يمثل واقعاً متنامياً. وينقل الكاتب عن خبراء أمنيين أن الفاعلين بالوكالة، ومجموعات الهاكتيفيزم، والأفراد المتوافقين مع الحكومات يمكن أن يلعبوا دوراً مهماً في تنفيذ هجمات سيبرانية غير مباشرة. ووفقاً لهذا الطرح، قد تلجأ إيران إلى مثل هذه الجماعات لممارسة ضغط سيبراني على أهداف حساسة داخل الولايات المتحدة دون تحمل المسؤولية المباشرة عن الهجمات. كما يشير المقال إلى تحذيرات صادرة عن جهات فدرالية أمريكية، من بينها وكالة الأمن السيبراني وأمن البنية التحتية (CISA)، التي أعلنت أن بعض المعدات المستخدمة في البنى التحتية الحيوية، مثل شبكات المياه والطاقة والخدمات العامة، تعرضت لمحاولات اختراق أو استغلال. ويرى الكاتب أن هذه الأنشطة أدت في بعض الحالات إلى تعطيلات تشغيلية وخسائر مالية، وأن هدفها العام يتمثل في إحداث عدم استقرار والضغط على الهياكل الحيوية للدولة. وفي جزء آخر، يؤكد خبراء الأمن أن البنى التحتية الحيوية، مثل المستشفيات وأنظمة المياه والطاقة والنقل، تبقى عرضة دائماً للتهديدات السيبرانية. ويُظهر المقال أنه حتى في غياب حرب سيبرانية مباشرة، فإن استخدام الشبكات الوكيلة والهجمات المتفرقة يمكن أن يزيد مستوى الخطر بشكل كبير. وفي الخلاصة، يرى الكاتب أن الوضع الحالي يمثل تحذيراً جدياً للولايات المتحدة وسائر الدول. ووفقاً للخبراء الذين استشهد بهم، قد لا تمتلك إيران حالياً القدرة على شن حرب سيبرانية واسعة ومباشرة، لكنها تستطيع من خلال الجماعات الوكيلة والهجمات المحدودة ممارسة ضغط ملحوظ على البنى التحتية الحساسة. ويخلص المقال إلى أن الفضاء السيبراني أصبح أحد الجبهات الرئيسية للتنافس والتوتر بين إيران والولايات المتحدة، وأن البنى التحتية الحيوية تقف في الخط الأمامي لهذا الصراع غير المباشر، وهو ما يستدعي، بحسب الكاتب، تعزيز الجاهزية وتقوية الدفاعات السيبرانية وتوسيع التعاون بين المؤسسات الحكومية والقطاع الخاص.

https://www.defenseone.com/threats/٤/٢٠٢٦/iran-hackers-

The Register

تزعم إيران أن الولايات المتحدة عطّلت شبكات الاتصالات أثناء الحرب باستخدام تكتيك الأبواب الخلفية

في ٢١ أبريل ٢٠٢٦، نُشر مقال بعنوان «تزعم إيران أن الولايات المتحدة عطّلت شبكات الاتصالات أثناء الحرب باستخدام أبواب خلفية» بقلم سايمون شاروود (Simon Sharwood) في موقع The Register. تركز الرواية الرئيسية للكاتب في هذا المقال على حرب السرديات في الفضاء السيبراني بين إيران والولايات المتحدة والصين، وتسعى إلى إظهار كيف تتحول الادعاءات غير المؤكدة في سياق الحرب السيبرانية إلى أدوات دعائية وسياسية. يرى الكاتب أن وسائل الإعلام الإيرانية، خلال الحرب الجارية، ادعت أن الولايات المتحدة تمكنت من تعطيل معدات الشبكات في إيران عبر «أبواب

خلفية» (Backdoors) أو شبكات مخترقة (Botnets). وتشير هذه التقارير إلى أن معدات من شركات Cisco وJuniper و Fortinet وMikroTik تعرضت لإعادة تشغيل مفاجئة أو خرجت من الخدمة، حتى في وقت كانت فيه إيران قد حدّت فعلياً من وصولها إلى الإنترنت العالمي. ومن وجهة نظر الإعلام الإيراني، فإن هذا لا يمكن تفسيره إلا بوجود أبواب خلفية مدمجة في الأجهزة أو البرمجيات تتيح للولايات المتحدة تعطيل الشبكات متى شاءت. ويشير الكاتب إلى أن هذه الادعاءات طُرحت غالباً في إطار سيناريوهات افتراضية يصعب التحقق منها. وقد ذهبت بعض الروايات الإيرانية إلى أبعد من ذلك، حيث افترضت أن الهجمات ربما نُفذت عبر إشارات الأقمار الصناعية أو من خلال تفعيل عن بُعد. كما طُرح سيناريو آخر يفترض وجود شبكة باتنت واسعة مزروعة داخل معدات الشبكات، تسمح بتنفيذ هجمات متزامنة على أجهزة متعددة. ومع ذلك، يؤكد الكاتب أنه لا يمكن التحقق من أي من هذه الادعاءات بشكل مستقل، خاصة في ظل القيود الشديدة أو شبه الانقطاع الكامل للإنترنت في إيران خلال تلك الفترة. وفي سياق متصل، يوضح المقال أن امتلاك الولايات المتحدة لقدرات متقدمة في العمليات السيبرانية أمر لا يمكن إنكاره، وقد أشار بعض المسؤولين العسكريين الأمريكيين إلى دور القيادة السيبرانية في العمليات الإقليمية. إلا أن الكاتب يشدد على أن امتلاك القدرة التقنية لا يعني صحة الادعاءات التي تطرحها وسائل الإعلام الإيرانية. ويخصص المقال جزءاً مهماً لرد الفعل الصيني، حيث يوضح أن وسائل الإعلام الحكومية الصينية استغلت هذه الادعاءات الإيرانية لتعزيز روايتها التي تصوّر «الغرب كتهديد رئيسي في الفضاء السيبراني». كما أن مؤسسات مثل المركز الوطني الصيني للاستجابة الطارئة لفيروسات الحاسوب (CVERC) دأبت على الادعاء بأن الولايات المتحدة تقوم بشكل منهجي بزرع أبواب خلفية في معدات الشبكات، بينما تعتبر الاتهامات الموجهة إلى الصين في مجال الهجمات السيبرانية جزءاً من خطاب سياسي. وفي هذا السياق، قامت وسائل الإعلام الصينية بتأييد ضمني للرواية الإيرانية واستخدامها لدعم مواقفها السياسية. ويؤكد الكاتب في هذا الجزء أن الحرب السيبرانية لم تعد مجرد صراع تقني، بل تحولت إلى ساحة تنافس في السرديات والدعاية السياسية، حيث يسعى كل طرف إلى تصوير الآخر باعتباره المعتدي الرئيسي وتوظيف الادعاءات التقنية لتحقيق شرعية سياسية. كما يتناول المقال وضع الإنترنت في إيران، مستشهداً بتقارير جهات مراقبة مثل NetBlocks، والتي تشير إلى أن البلاد كانت تعاني من انقطاع واسع وطويل الأمد في الإنترنت خلال تلك الفترة. وقد جعل هذا الوضع التحقق من الادعاءات المتعلقة بالهجمات السيبرانية أمراً بالغ الصعوبة أو شبه مستحيل. وتشير بعض التقارير إلى أن الوصول إلى الإنترنت كان متاحاً بشكل انتقائي لفئات محددة فقط. وفي الخلاصة، يرى الكاتب أننا أمام بيئة معقدة تتداخل فيها «الادعاءات غير المؤكدة، والحرب المعلوماتية، والتنافس الجيوسياسي في الفضاء السيبراني». فمن جهة، تدعي إيران تعرضها لهجمات سيبرانية أمريكية عبر أبواب خلفية، ومن جهة أخرى تستخدم الصين هذه الرواية لتعزيز خطابها المناهض للولايات المتحدة. غير أن الكاتب يؤكد أنه لا توجد أدلة قاطعة ومستقلة تثبت هذه الادعاءات، وأن جزءاً كبيراً من هذه القضية يندرج ضمن الحرب النفسية والمعلوماتية أكثر من كونه واقعاً تقنياً مثبتاً. ويخلص المقال إلى أن الفضاء السيبراني أصبح اليوم ميداناً لصراع السرديات، حيث تتداخل الحقيقة التقنية مع الادعاءات السياسية والدعاية الحكومية، ويصبح التمييز بين الواقع والرواية أمراً بالغ الصعوبة، خاصة في ظروف الحرب وانقطاع الاتصالات.

https://www.theregister.com/٢١/٠٤/٢٠٢٦/iran_claims_

Industrial Cyber

تحذر شركة Resecurity من أن الحرب الإيرانية دخلت مرحلة متعددة المجالات، حيث أصبحت العمليات السيبرانية والعسكرية مترابطة ومتشابكة

في ٢٤ مارس ٢٠٢٦، نُشر مقال بعنوان «تحذّر شركات الأمن السيبراني من أن الحرب الإيرانية دخلت مرحلة متعددة المجالات، حيث أصبحت العمليات السيبرانية والعسكرية مترابطة» بقلم آنا ريبيرو على موقع Industrial Cyber. تركز الرواية الرئيسية للكاتبة في هذا المقال على أن الصراعات المرتبطة بإيران لم تعد مجرد حرب عسكرية تقليدية، بل تحولت إلى حرب مركبة متعددة الطبقات، تتداخل فيها العمليات السيبرانية والهجمات العسكرية والحرب النفسية وأنشطة مجموعات الهاكتيفيزم بشكل متزامن ومنسق. ترى الكاتبة أنه بعد الهجوم المشترك للولايات المتحدة وإسرائيل على إيران في فبراير ٢٠٢٦، تصاعد مستوى التوتر بشكل ملحوظ، ولم تقتصر هذه الهجمات على الجانب العسكري (الصواريخ والطائرات المسيّرة)، بل ترافقت أيضاً مع عمليات سيبرانية وإلكترونية تهدف إلى إضعاف شبكات الاتصالات، وجمع المعلومات، وتعطيل منظومات القيادة العسكرية الإيرانية. وفي المقابل، دخلت مجموعات قرصنة مرتبطة بإيران، إلى جانب مجموعات متوافقة مع الغرب، في دورة من المواجهة الرقمية استهدفت البنى التحتية الحيوية والمواقع الحكومية والأنظمة الصناعية. وتتابع الكاتبة أن مجموعات الهاكتيفيزم أصبحت لاعباً بارزاً في هذه الحرب. فقد نفذت مجموعات إيرانية مثل Cyber Islamic Resistance وFatimion Cyber Team وCyber Fattah عمليات تشمل هجمات حجب الخدمة (DDoS)، واختراق المواقع، وسرقة البيانات، وجمع المعلومات. وفي المقابل، استهدفت مجموعات موالية للغرب مواقع وتطبيقات مرتبطة بإيران بهدف إضعاف الروايات الإعلامية والاجتماعية للحكومة الإيرانية. وتؤكد الرواية الرئيسية للمقال أن هذه الحرب السيبرانية باتت منسقة بشكل مباشر مع العمليات العسكرية. فعلى سبيل المثال، تُستخدم العمليات السيبرانية لتحديد الأهداف العسكرية، وتقييم نتائج الضربات، والتمهيد لهجمات ميدانية لاحقة. وقد أدى هذا التداخل إلى تلاشي الحدود بين الحرب الرقمية والحرب التقليدية، وظهور ما يمكن وصفه بـ«الحرب الهجينة». وفي جزء آخر، توضح الكاتبة أن الأنشطة السيبرانية تُنفذ غالباً عبر مجموعات بالوكالة وهاكتيفيست، نظراً لتراجع القدرات السيبرانية المباشرة لإيران بسبب قيود البنية التحتية وانقطاع أو تقييد الإنترنت الداخلي. لذلك تعتمد إيران بشكل أكبر على شبكات غير مركزية ومجموعات خارجية متحالفة معها. ومع ذلك، فإن هذه المجموعات تميل إلى تنفيذ هجمات محدودة نسبياً مثل هجمات DDoS والاختراقات السطحية وأعمال التخريب الرقمي، والتي تكون صاخبة إعلامياً لكنها محدودة التأثير عملياً. كما تشير الكاتبة إلى دور الذكاء الاصطناعي والحرب المعلوماتية، حيث تُستخدم أدوات الذكاء الاصطناعي لإنتاج المحتوى، ونشر المعلومات المضللة، وتنفيذ عمليات نفسية تستهدف التأثير على الرأي العام ومعنويات الخصم. ومن الأمثلة على ذلك نشر مقاطع فيديو مزيفة من ساحات القتال أو ترويج شائعات حول هجمات عسكرية. وتوضح المقالة أيضاً أن العديد من الهجمات السيبرانية الأخيرة شملت هجمات DDoS، وتخريب مواقع إلكترونية، ومحاولات لاختراق أنظمة صناعية، لكنها غالباً كانت منخفضة المستوى تقنياً أو متفرقة، وتركز أكثر على التأثير النفسي والإعلامي بدلاً من تحقيق نتائج تشغيلية ملموسة. كما استخدمت بعض المجموعات خدمات هجومية مؤجرة (stresser services) وشبكات باتنت بسيطة لزيادة حجم الحركة الضارة. وتشير الرواية كذلك إلى أن بعض الهجمات استهدفت بنى تحتية حساسة مثل الطاقة والنقل وحتى شركات دفاعية في دول مختلفة، إلا أن كثيراً منها كان ذا طابع انتهازي أكثر منه عمليات منسقة ومتقدمة. كما حاولت بعض المجموعات استغلال بيانات مسروقة وثغرات معروفة للتسلل إلى الأنظمة الصناعية وكاميرات المراقبة. وفي الخلاصة، ترى الكاتبة أن الحرب المرتبطة بإيران دخلت مرحلة تلاشت فيها الحدود بين الحرب السيبرانية والعسكرية والمعلوماتية. وقد أدى ذلك إلى مشاركة أطراف متعددة—من الدول إلى مجموعات الهاكتيفيزم وحتى مجرمي الإنترنت—في ساحة واحدة. ومع ذلك، تؤكد المقالة أن تأثير العديد من هذه الهجمات لا يزال محدوداً، وغالباً ما يقتصر على إحداث اضطرابات قصيرة الأمد أو التأثير النفسي والإعلامي. وفي النهاية، يخلص المقال إلى أن العالم دخل مرحلة «الحرب الرقمية الهجينة»، حيث تتكامل العمليات السيبرانية والإعلامية والعسكرية والذكاء الاصطناعي لخدمة الأهداف الجيوسياسية، وتُعد إيران إحدى النقاط المحورية في هذا التحول المعقد.

https://industrialcyber.co/critical-infrastructure/resecurity-warns-that-

CNN

داخل الحرب النفسية التي تشنها إيران ضد خصومها

في ١٦ أبريل ٢٠٢٦، نُشر مقال بعنوان «في انتظار الموت: داخل الحرب النفسية التي تشنها إيران ضد خصومها» بقلم مصطفى سالم (Mostafa Salem). تركز الرواية الرئيسية للكاتب في هذا المقال على تشكّل حرب مركبة ومتعددة الطبقات تقودها إيران، حيث يتم توظيف «الحرب النفسية، والعمليات المعلوماتية، والهجمات السيبرانية» إلى جانب التحركات العسكرية للضغط على الخصوم الإقليميين والدوليين. يرى الكاتب أنه خلال الحرب الأخيرة بين إيران وإسرائيل والولايات المتحدة، لم يقتصر ميدان القتال على الصواريخ والطائرات المسيّرة، بل ظهر أيضاً جبهة خفية لكنها شديدة التأثير في المجالين النفسي والمعلوماتي.

وفي هذا الإطار، سعت إيران والجماعات المرتبطة بها، من خلال إرسال رسائل تهديد، وتنفيذ عمليات تصيّد (phishing)، وشن هجمات سيبرانية، ونشر معلومات مضللة، إلى خلق أجواء من الخوف وانعدام الأمن في دول المنطقة. ويشير الكاتب إلى أمثلة محددة، منها إرسال رسائل نصية مزيفة باسم جهات رسمية مثل وزارة الداخلية في الإمارات، تطلب من المواطنين الإبلاغ عن «حوادث أمنية» محتملة. وقد وُصفت هذه الرسائل، التي تبين أنها مزيفة، بأنها جزء من عملية نفسية أوسع تهدف إلى تقويض الثقة بالمؤسسات الرسمية. كما أفادت التقارير بأن حجم الهجمات السيبرانية وعمليات التصيّد من قبل مجموعات مرتبطة بإيران ارتفع بشكل كبير في الأيام الأولى من الحرب، ليصل في بعض الحالات إلى مئات الآلاف من الهجمات يومياً. وتؤكد الرواية الرئيسية للمقال أن إيران، بدلاً من التركيز فقط على القوة العسكرية، عملت بشكل ممنهج على «إضعاف المعنويات، وبث الخوف، وزعزعة الاستقرار النفسي» في دول الخليج. وفي هذا السياق، تُعد الرسائل التهديدية الموجهة إلى المواطنين الإسرائيليين، والتحذيرات الزائفة بالإخلاء، ونشر قوائم أهداف تشمل شركات وجامعات غربية، جزءاً من استراتيجية أوسع للضغط النفسي. وفي جزء آخر، يتناول المقال الهجمات السيبرانية التي استهدفت البنى التحتية الاقتصادية والحيوية في المنطقة. ففي الأردن، وُجهت اتهامات لمجموعات مرتبطة بإيران بمحاولة تعطيل أنظمة تخزين المواد الغذائية. كما شهدت الإمارات والبحرين هجمات سيبرانية أدت إلى اضطرابات في الأنظمة المصرفية والخدمات المالية. ويرى الكاتب أن هذه الهجمات، رغم محدوديتها أحياناً، تهدف أساساً إلى إحداث تأثير نفسي واقتصادي واسع. كما يشير المقال إلى محاولات اختراق أنظمة المراقبة والكاميرات الأمنية، حيث سعت مجموعات قرصنة مرتبطة بإيران إلى الوصول إلى صور الكاميرات في إسرائيل ودول الخليج، لاستخدامها في تحديد الأهداف أو تقييم أضرار الضربات العسكرية، ما يعكس تداخلاً متزايداً بين الحرب السيبرانية والعمليات العسكرية. وتتناول الرواية أيضاً مسألة التحكم في المعلومات والرقابة، إذ قامت بعض الحكومات العربية باعتقال أشخاص نشروا صوراً أو معلومات تتعلق بالحرب، في محاولة لمنع تسريب بيانات حساسة. وقد أدى ذلك إلى انتشار حالة من الرقابة الذاتية بين المواطنين والصحفيين. ويمتد نطاق الهجمات السيبرانية، بحسب المقال، إلى خارج الشرق الأوسط، حيث تم استهداف شركات أمريكية، وتسريب رسائل بريد إلكتروني، ومهاجمة بنى تحتية في مجالات الصحة والطاقة. ويؤكد الكاتب أن لهذه العمليات بعداً نفسياً قوياً يهدف إلى تضخيم صورة القوة السيبرانية الإيرانية وبث الشعور بعدم الأمان لدى الخصوم. ومع ذلك، يشير الكاتب إلى أن العديد من الخبراء يرون أن القيود على الإنترنت داخل إيران قد حدّت من قدراتها السيبرانية، حيث أدى قطع أو تقييد الإنترنت إلى تقليل القدرة على التنسيق وتنفيذ عمليات معقدة، مما دفعها للاعتماد بشكل أكبر على مجموعات بالوكالة خارج البلاد. وفي الخلاصة، يرى الكاتب أن الهدف الرئيسي لإيران في هذه الحرب المركبة ليس بالضرورة تحقيق نصر عسكري مباشر، بل خلق «الخوف، وعدم الاستقرار، وحالة من عدم اليقين» لدى الخصوم. ويعتقد الخبراء أن مثل هذه العمليات يمكن أن تُحدث تأثيرات سياسية ونفسية كبيرة حتى دون وقوع أضرار مادية واسعة، من خلال تقويض ثقة الجمهور بقدرة الحكومات على توفير الأمن. ويخلص المقال إلى أن الحروب الحديثة لم تعد تقتصر على ساحات القتال التقليدية، بل أصبحت تُخاض في العقول، وشبكات الاتصال، والفضاء المعلوماتي، حيث تُعد إيران أحد أبرز الفاعلين في توظيف الأدوات النفسية والسيبرانية لتحقيق أهدافها الاستراتيجية في المنطقة.

https://edition.cnn.com/١٦/٠٤/٢٠٢٦/middleeast/iran-war-psychology-israel-

New York Times

على الرغم من وقف إطلاق النار، لم يتوقف القراصنة الإيرانيون عن نشاطهم

في ١٦ أبريل ٢٠٢٦، نُشر مقال بعنوان «على الرغم من وقف إطلاق النار، لم يتوقف القراصنة الإيرانيون عن نشاطهم» بقلم جوليان إيه. بارنز وداستن وولتز في صحيفة The New York Times. تركز الرواية الرئيسية للكاتبين في هذا المقال على أن الحرب السيبرانية مستمرة حتى بعد التوقف المؤقت للعمليات العسكرية بين إيران والولايات المتحدة وإسرائيل، وأن إيران تستخدم هذا الفضاء للحفاظ على الضغط والاستعداد لمراحل لاحقة من الصراع. يرى الكاتبان أنه رغم توقف

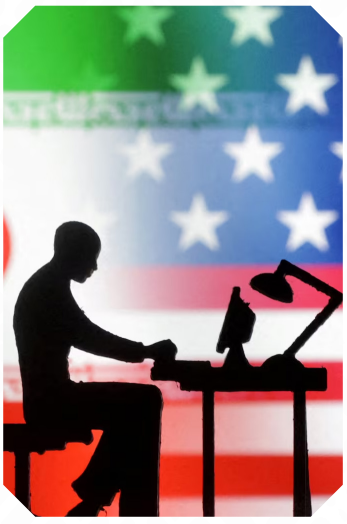
تبادل الصواريخ والهجمات العسكرية في المنطقة مؤقتاً، فإن الأنشطة السيبرانية الإيرانية لم تتراجع، بل استمرت في بعض المجالات وتغيرت طبيعتها. وفي هذا السياق، تستخدم إيران الحرب السيبرانية كأداة للحفاظ على «الضغط الاستراتيجي» على الولايات المتحدة وإسرائيل، مع إبقاء نفسها مستعدة لاحتمال انهيار وقف إطلاق النار أو تعثر المفاوضات. ويشرح المقال أنه خلال الحرب الأخيرة، استخدمت إيران مزيجاً من الهجمات العسكرية، وعمليات التضليل المعلوماتي، والهجمات السيبرانية منخفضة وعالية المستوى، بهدف إرباك إسرائيل وإحداث اضطرابات في بعض البنى التحتية الحيوية في الولايات المتحدة. ومن الأمثلة التي يوردها المقال الهجوم السيبراني على شركة المعدات الطبية Stryker، والذي أدى إلى تعطيل واسع في عملياتها العالمية. كما يُتهم بعض الجماعات المرتبطة بإيران بنشر رسائل بريد إلكتروني وصور مسروقة من حسابات مرتبطة بمسؤولين أمنيين أمريكيين. وتشير الرواية الرئيسية إلى أنه بعد بدء وقف إطلاق النار، غيّرت إيران استراتيجيتها. فبدلاً من العمليات العلنية والصاخبة، أصبح التركيز على «التسلل الصامت» والتجسس السيبراني. أي أن الهدف لم يعد فقط إحداث اضطراب فوري، بل بناء وصول طويل الأمد إلى الشبكات الحساسة والبنى التحتية الحيوية. ويؤكد الكاتبان أن الأهداف السيبرانية الإيرانية تشمل أفراداً مرتبطين بالحكومتين الأمريكية والإسرائيلية، إضافة إلى بنى تحتية حيوية مثل أنظمة المياه والكهرباء في الشرق الأوسط والولايات المتحدة. ووفقاً للمقال، فإن هذه الجهود تهدف إلى خلق «رافعة ضغط مستقبلية» يمكن استخدامها في حال فشل المفاوضات أو استئناف الحرب. وفي جزء آخر، يقارن المقال القدرات السيبرانية الإيرانية بدول مثل الصين وروسيا. ويشير إلى أن إيران أقل تطوراً من الناحية التقنية، لكنها تظل لاعباً مهماً في الحرب السيبرانية بسبب شبكتها الواسعة واللامركزية من القراصنة المرتبطين بها. كما تُوصف بأنها أكثر تقلباً وغير متوقعة مقارنة بالصين وروسيا، خاصة عند شعورها بالتهديد السياسي أو العسكري. كما يوضح المقال أن إيران تركز بشكل خاص على أهداف أضعف وأقل حماية، مثل المنشآت البلدية والشركات الصغيرة والمؤسسات المحلية، بما في ذلك أنظمة المياه والطاقة وشركات الاستشارات المالية المرتبطة بالأفراد الأثرياء. وتهدف هذه الهجمات إلى خلق نفوذ غير مباشر والوصول إلى معلومات حساسة عبر شبكات شخصية وغير رسمية. ويشير المقال إلى انخفاض نسبي في بعض الهجمات السيبرانية داخل الولايات المتحدة بعد وقف إطلاق النار، لكنه يؤكد أن هذا لا يعني نهاية التهديد. بل إن إيران تتحول من الهجمات العلنية إلى التسلل طويل الأمد والبقاء داخل الشبكات، بهدف الحفاظ على وصول خفي يمكن استخدامه لاحقاً. كما يتناول المقال نشاط مجموعة القرصنة Handala المنسوبة إلى إيران، والتي نفذت هجمات ضد إسرائيل وبعض دول المنطقة، بما في ذلك اختراق حسابات أفراد عسكريين وأمنيين ونشر بياناتهم. ويشير الكاتبان إلى أن هذه المجموعة تُقدَّم ككيان هاكتيفيست مستقل، لكنها في الواقع مرتبطة بأجهزة الاستخبارات الإيرانية. وفي الجزء الأخير، يسلط المقال الضوء على زيادة النشاط السيبراني الإيراني في منطقة الخليج، حيث تشير تقارير شركات الأمن السيبراني إلى ارتفاع ملحوظ في الهجمات بعد وقف إطلاق النار، إلى جانب استمرار استهداف إسرائيل. وفي الخلاصة، يرى الكاتبان أن وقف إطلاق النار لا يعني نهاية الحرب، بل مجرد تغيير في شكلها. فقد انتقل الصراع من المجال المادي إلى المجال الرقمي والمعلوماتي، حيث يستمر بدرجة عالية من النشاط. ومن هذا المنظور، تحاول إيران استغلال هذه المرحلة الهادئة نسبياً لإعادة بناء قدراتها السيبرانية، والتغلغل في الشبكات المستهدفة، والاستعداد لجولة جديدة من المواجهة. ويخلص المقال إلى أن الحروب الحديثة لم تعد تنتهي بوقف إطلاق النار في الميدان التقليدي، لأن الفضاء السيبراني يبقى نشطاً دائماً. وتُقدَّم إيران كمثال رئيسي على ذلك، إذ تواصل الحرب في البعد الرقمي حتى في أوقات الهدوء العسكري النسبي، مستخدمة إياه كأداة دائمة للضغط الجيوسياسي.

https://www.nytimes.com/١٦/٠٤/٢٠٢٦/us/politics/iran-war-hacking-

The Conversation

كيف يشكّل القراصنة الإيرانيون تهديداً للبنية التحتية الحيوية في الولايات المتحدة

في ٢ أبريل ٢٠٢٦ (مع تحديث في ٩ أبريل ٢٠٢٦)، نُشر مقال بعنوان «كيف يشكّل القراصنة الإيرانيون تهديداً للبنية التحتية الحيوية في الولايات المتحدة». تركز الرواية الرئيسية للكاتب في هذا المقال على أن الحرب السيبرانية بين إيران والولايات المتحدة ليست مجرد سلسلة من الهجمات المتفرقة، بل هي جزء من نمط بنيوي في «الحرب السيبرانية الحديثة»، يهدف إلى إنشاء وصول خفي، واختراق طويل الأمد، والتهيئة لاضطرابات مستقبلية في البنية التحتية الحيوية. يرى الكاتب أن المجموعات المرتبطة بإيران، مثل مجموعة القرصنة Handala، نفذت خلال التوترات الأخيرة في الشرق الأوسط هجمات ضد شركات وبنى تحتية حساسة في الولايات المتحدة. ومن الأمثلة المذكورة الهجوم على شركة المعدات الطبية Stryker في ولاية ميشيغان بتاريخ ١١ مارس ٢٠٢٦، والذي أدى إلى تعطيل الأنظمة الداخلية، بما في ذلك عمليات الطلب والإنتاج والنقل في الشركة. ومن وجهة نظر الكاتب، يوضح هذا الهجوم أن المسافة الجغرافية في الحرب السيبرانية لم تعد ذات أهمية، وأن الصراعات الإقليمية يمكن أن تؤثر بسرعة على شركات وبنى تحتية بعيدة. ويؤكد المقال أن البنية التحتية الحيوية في الولايات المتحدة لا تقتصر على المنشآت المباشرة مثل محطات الطاقة أو شبكات المياه، بل تشمل أيضاً شبكة معقدة من شركات الخدمات ومزودي تكنولوجيا المعلومات ومراكز البيانات وسلاسل الإمداد. وبالتالي، فإن استهداف شركة خاصة يمكن أن يؤثر بشكل غير مباشر على أنظمة حيوية مثل المستشفيات أو النقل. وتتمثل الرواية الرئيسية في أن الهجمات السيبرانية في سياقات التوتر الجيوسياسي لا تُصمم فقط لإحداث ضرر فوري، بل تهدف أساساً إلى إنشاء «وصول دائم» و«رافعة ضغط مستقبلية». ويوضح الكاتب أن الوصول إلى الشبكات في منطق الحرب السيبرانية يشبه امتلاك «مفاتيح دخول»، إذ إن التسلل الخفي والحفاظ على الوجود داخل النظام يتيحان لاحقاً سرقة البيانات أو إحداث اضطرابات أو ممارسة ضغط سياسي. وفي سياق متصل، يشير المقال إلى نماذج مثل مجموعة Volt Typhoon لإظهار أن هذا النمط من النشاط لا يقتصر على إيران، بل تستخدمه أيضاً قوى أخرى. وقد اعتمدت هذه المجموعة على أساليب تُعرف باسم "living-off-the-land"، ما مكنها من البقاء داخل الشبكات باستخدام أدوات النظام الداخلية لإخفاء أنشطتها. وتؤكد الرواية أن الخطر الحقيقي يتمثل في هذا النوع من الاختراق غير المرئي الذي يستمر في الخلفية دون اكتشافه. كما يشرح المقال المراحل القياسية للهجمات السيبرانية الحكومية أو شبه الحكومية: يبدأ الهجوم بالتصيّد أو استغلال الثغرات للدخول إلى النظام، ثم يتحرك المهاجمون بشكل خفي داخل الشبكة، ويرفعون صلاحياتهم، ويؤسسون حالة من «الثبات» (persistence) تتيح لهم العودة حتى بعد اكتشاف الهجوم. وفي المرحلة النهائية، يمكن أن تتحول العملية إلى سرقة بيانات أو تعطيل عمليات أو حتى حرب نفسية. ويستعرض المقال أيضاً أمثلة تاريخية مثل هجوم Shamoon عام ٢٠١٢، وهجوم مكتب إدارة الموارد البشرية الأمريكي عام ٢٠١٥، وهجوم Sony Pictures عام ٢٠١٤، لإظهار أن أهداف الهجمات السيبرانية لا تقتصر على التدمير، بل قد تشمل السرقة أو الرسائل السياسية. كما يشير الكاتب إلى أن الحكومة الأمريكية تمتلك أدوات دفاعية متعددة مثل وكالة الأمن السيبراني وأمن البنية التحتية (CISA)، ومكتب التحقيقات الفيدرالي (FBI)، ووكالة الأمن القومي (NSA)، والتي تعمل على رفع مستوى الجاهزية السيبرانية عبر التحذيرات والتعاون مع القطاع الخاص. ومع ذلك، يؤكد المقال أن طبيعة البنية التحتية الأمريكية، التي تعتمد بشكل كبير على الشركات الخاصة، تجعل الدفاع السيبراني مسؤولية مشتركة ومعقدة. ويضيف المقال أن التحديات ما زالت قائمة، بما في ذلك نقص الموارد، وتفاوت مستويات الأمن بين الشركات، وصعوبة كشف المهاجمين الخفيين، ما يعني أنه لا يوجد نظام دفاعي محصّن بالكامل. وفي الخلاصة، يرى الكاتب أن القراصنة المرتبطين بإيران يمثلون جزءاً من نمط أوسع في الحرب السيبرانية الحديثة، حيث لا يقتصر الهدف على الإضرار الفوري، بل يشمل إنشاء اختراقات طويلة الأمد، وحصول على وصول خفي، والاستعداد لأزمات مستقبلية. ومن هذا المنظور، أصبحت الهجمات السيبرانية أداة لـ«إظهار القوة غير المرئية» أكثر من كونها مجرد وسيلة للتدمير. ويختتم المقال بأن الحروب الحديثة لم تعد محصورة في ساحات القتال التقليدية، بل أصبحت هناك حرب صامتة تدور داخل الشبكات الرقمية، حيث يصبح التسلل والاستمرارية والوصول أكثر أهمية من التدمير الفوري، وتصبح البنية التحتية الحيوية الأمريكية في خط المواجهة الأمامي لهذا الصراع غير المرئي.



https://theconversation.com/how-iranian-hackers-pose-a-threat-to-

CSIS

تصاعد التوتر مع إيران يفاقم التهديدات السيبرانية ضد البنية التحتية للطاقة في الولايات المتحدة

في ٢ أبريل ٢٠٢٦، نُشر مقال بعنوان «تصاعد التوتر مع إيران يفاقم التهديدات السيبرانية ضد البنية التحتية للطاقة في الولايات المتحدة» بقلم ليزلي أبرامز (Leslie Abrahams) ولورين ويليامز (Lauryn Williams). تركز الرواية الرئيسية للكاتبتين في هذا المقال على أن البنية التحتية للطاقة في الولايات المتحدة، باعتبارها من أكثر القطاعات حيوية وحساسية في الوقت نفسه، أصبحت تواجه تهديدات سيبرانية وجيوسياسية متزايدة، وقد تفاقمت هذه التهديدات في سياق التوترات بين إيران والولايات المتحدة وإسرائيل. ترى الكاتبتان أن الطاقة لطالما كانت أداة ضغط جيوسياسي عبر التاريخ، من العقوبات والحصارات النفطية إلى الهجمات المادية على منشآت الطاقة. لكن في السياق الحالي، تغير شكل هذه التهديدات، وأصبحت الهجمات السيبرانية بديلاً أو مكملاً للهجمات التقليدية في الحروب الحديثة. وفي هذا الإطار، يشير المقال إلى أن إيران، إلى جانب قوى أخرى مثل الصين وروسيا، تستخدم الهجمات السيبرانية للتسلل، وإحداث الاضطراب، وتهيئة بيئة للأزمات المستقبلية. وتوضح الرواية أنه خلال التوترات الأخيرة في الشرق الأوسط، بما في ذلك المواجهات بين إيران والولايات المتحدة وإسرائيل، نُفذت هجمات محدودة نسبياً على البنية التحتية السيبرانية. ورغم أن هذه الهجمات أقل تعقيداً مقارنة بتلك المنسوبة إلى قوى كبرى أخرى، فإنها لا تزال قادرة على إحداث اضطرابات وجمع معلومات حساسة. ومن الأمثلة المذكورة الهجوم على شركة Stryker، والذي يوضح كيف يمكن حتى للشركات غير العسكرية ضمن سلاسل التوريد الطبية والصناعية أن تصبح أهدافاً. وتؤكد الرواية الرئيسية أن التهديد السيبراني ضد البنية التحتية للطاقة في الولايات المتحدة ليس مجرد احتمال نظري، بل هو تهديد حقيقي ومتزايد. وتشير الكاتبتان إلى أن شبكة الطاقة الأمريكية واسعة جداً، وغير مركزية، وقديمة في بعض أجزائها، مما يجعلها هدفاً جذاباً للهجمات السيبرانية. وتشمل هذه الشبكة آلاف محطات الطاقة، ومئات آلاف الكيلومترات من خطوط النقل، وملايين نقاط الاتصال الرقمية التي يمكن أن تشكل نقاط دخول للمهاجمين. كما يسلط المقال الضوء على الطبيعة المجزأة لصناعة الطاقة في الولايات المتحدة، حيث يؤدي تعدد الشركات والجهات المستقلة واختلاف مستويات الأمن السيبراني بينها إلى صعوبة فرض معايير موحدة للحماية. إضافة إلى ذلك، فإن الترابط الكبير بين أجزاء الشبكة يجعل أي هجوم على جزء صغير منها قادراً على إحداث تأثيرات متسلسلة على النظام بأكمله. وتشير الرواية أيضاً إلى مشكلة تقادم البنية التحتية، إذ إن العديد من خطوط الأنابيب ومحطات الطاقة وشبكات النقل تعود لعقود مضت ولم تُصمم للبيئة الرقمية الحديثة. وغالباً ما تفتقر هذه الأنظمة إلى أدوات الأمن السيبراني المتقدمة، كما أن تحديثها قد يؤدي أحياناً إلى إدخال ثغرات جديدة. وفي جزء مهم من المقال، تتناول الكاتبتان مفهوم «التموضع المسبق (pre-positioning)»، والذي يشير إلى التسلل الخفي إلى الشبكات الحيوية دون إحداث ضرر فوري. وفي هذا السياق، تُعد مجموعات مثل Volt Typhoon مثالاً على هذا النهج، حيث تعمل على الحفاظ على وصول طويل الأمد إلى الأنظمة بهدف استخدامه لاحقاً في أوقات الأزمات. وتشير الرواية إلى أن إيران تتبع نمطاً مشابهاً، وإن كان على نطاق مختلف. كما يناقش المقال أهداف الهجمات السيبرانية، والتي تشمل سرقة البيانات، والتجسس الصناعي، وإحداث تعطيل مباشر، أو حتى إرسال رسائل سياسية. ويستشهد المقال بهجوم Colonial Pipeline عام ٢٠٢١ لإظهار كيف يمكن لهجوم سيبراني واحد أن يؤدي إلى آثار اقتصادية واسعة مثل نقص الوقود وارتفاع الأسعار واضطرابات في النقل. وتوضح الرواية أيضاً أن قطاع الطاقة يُعد من أكثر القطاعات استهدافاً في الولايات المتحدة، حيث يتم تسجيل آلاف محاولات الاختراق أسبوعياً. ورغم أن معظم هذه المحاولات لا تنجح، فإن حجمها الكبير يعكس خطورة التهديد المستمر. وفي الختام، تؤكد الكاتبتان أن مواجهة هذه التهديدات تتطلب تعاوناً وثيقاً بين الحكومة والقطاع الخاص، نظراً لأن معظم البنية التحتية للطاقة مملوكة لشركات خاصة. كما تدعو المقالة إلى تعزيز معايير الأمن السيبراني، وتحسين تبادل المعلومات، وتطوير الكفاءات البشرية في هذا المجال. وتخلص الرواية إلى أن البنية التحتية للطاقة في الولايات المتحدة تواجه مزيجاً من الضعف المادي والرقمي، وأن التوترات الجيوسياسية، وخاصة تلك المرتبطة بإيران، تزيد من حدة هذا التهديد. ومن هذا المنظور، لا يتمثل الخطر الرئيسي في الهجمات المباشرة فقط، بل في عمليات التسلل الخفية والوصول طويل الأمد والاستعداد للأزمات المستقبلية، مما يجعل الحرب السيبرانية جزءاً دائماً من التنافس بين القوى العالمية.

https://www.csis.org/analysis/iran-conflict-heightens-cyber-threats-us-

القيادة السيبرانية الأمريكية

تحذيرات عالمية من الحرب السيبرانية الإيرانية وتهديدها للبنية التحتية الحيوية في الولايات المتحدة

في ٧ أبريل ٢٠٢٦، نشرت عدة جهات رسمية في الولايات المتحدة، تشمل مكتب التحقيقات الفيدرالي (FBI)، ووكالة الأمن السيبراني وأمن البنية التحتية (CISA)، ووكالة الأمن القومي (NSA)، ووزارة الطاقة، ووكالة حماية البيئة، والقيادة السيبرانية للجيش الأمريكي، تقريراً مشتركاً بعنوان: «Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure». ويُعد هذا التقرير، الصادر تحت الرقم ٠٩٧A-AA٢٦ وبمستوى تصنيف TLP:CLEAR، أحد أبرز التحذيرات الأمنية لعام ٢٠٢٦ بشأن التهديدات السيبرانية ضد البنية التحتية الحيوية في الولايات المتحدة.

تتمثل الرواية الرئيسية في التقرير في أن مجموعات قرصنة مرتبطة بإيران (Iran-affiliated APT actors) تنفذ عمليات تسلل واستغلال بشكل ممنهج لأنظمة صناعية متصلة بالإنترنت، وخاصة وحدات التحكم المنطقي القابلة للبرمجة (PLC)، التي تنتجها شركات مثل Rockwell Automation / Allen-Bradley. ويشير التقرير إلى أن هذه الهجمات لا تقتصر على قطاع واحد، بل تم رصدها في عدة قطاعات حيوية تشمل المياه والصرف الصحي والطاقة والخدمات العامة التابعة للحكومات المحلية في الولايات المتحدة. ويؤكد التقرير أن هذه العمليات لا تهدف إلى التخريب البسيط فقط، بل تُنفذ ضمن مراحل متعددة. ووفق تحليل الجهات المعدّة للتقرير، يبدأ المهاجمون بالدخول إلى الشبكات الصناعية عبر الأنظمة المتصلة بالإنترنت، ثم يحصلون على وصول إلى ملفات المشاريع الخاصة بوحدات PLC، وفي المرحلة التالية يقومون بتعديل البيانات المعروضة في أنظمة HMI وSCADA. وقد أدت هذه العمليات إلى اضطرابات تشغيلية، وفي بعض الحالات إلى خسائر مالية. وتصف الرواية هذه الأنشطة بأنها جزء من تكتيكات حرب سيبرانية منظمة تهدف إلى زعزعة الاستقرار والضغط على البنية التحتية الحيوية للولايات المتحدة. ويشير التقرير أيضاً إلى أن هذه الجهات تستخدم بنى تحتية خارجية لتنفيذ الهجمات، وتستفيد من برمجيات هندسية صناعية مثل Studio ٥٠٠٠ Logix Designer للوصول إلى الأنظمة المستهدفة. كما يوضح أن الاتصالات الخبيثة تتم غالباً عبر منافذ صناعية محددة مثل ٤٤٨١٨ و٢٢٢٢ و١٠٢ و٢٢ و٥٠٢، وفي بعض الحالات يتم استخدام أدوات وصول عن بُعد مثل Dropbear SSH للحفاظ على وجود دائم داخل الأنظمة المخترقة. ومن النقاط المهمة في الرواية مفهوم «التموضع المسبق» (pre-positioning)، أي أن الهدف من بعض عمليات الاختراق ليس إحداث ضرر فوري، بل إنشاء وصول دائم إلى الشبكات الحيوية لاستخدامه في أوقات الأزمات المستقبلية. ويؤكد التقرير أن هذا يعكس تحول الفضاء السيبراني إلى ساحة دائمة للتنافس الجيوسياسي.

كما يشير التقرير إلى سوابق تاريخية لهذه الهجمات، مثل مجموعة CyberAv٣ngers المرتبطة بالحرس الثوري الإيراني، والتي استهدفت في سنوات سابقة (٢٠٢٣ و٢٠٢٤) أنظمة المياه والبنية التحتية الصناعية. ويعتبر التقرير أن الهجمات الحالية امتداد لهذا النمط ولكن بدرجة أعلى من التعقيد والاستمرارية. وفي تحليل التهديد، يؤكد معدّو التقرير أن الهدف لا يقتصر على الضرر التقني، بل يشمل أيضاً إحداث الخوف، وتقويض الثقة، والتأثير على إدارة البنى التحتية. كما يحذر التقرير من أن الوصول إلى ملفات مشاريع PLC قد يُستخدم لاحقاً لتنفيذ هجمات أكثر تنسيقاً وتأثيراً. وتتضمن التوصيات المقدمة للجهات الأمريكية منع توصيل PLC مباشرة بالإنترنت، واستخدام جدران حماية وبوابات آمنة، وتفعيل المصادقة متعددة العوامل، ومراقبة سجلات الشبكة للكشف عن النشاطات المشبوهة، إضافة إلى ضرورة الاحتفاظ بنسخ احتياطية غير متصلة بالإنترنت للأنظمة الصناعية. وفي الخلاصة، يرى التقرير أن إيران والجماعات المرتبطة بها تنفذ استراتيجية سيبرانية طويلة الأمد ضد البنية التحتية الحيوية الأمريكية، تشمل التسلل الخفي، وجمع المعلومات، والتهيئة لاضطرابات مستقبلية. ويؤكد أن التهديد الحقيقي لا يكمن فقط في تنفيذ الهجمات، بل في وجود المهاجمين بشكل غير مرئي داخل الشبكات الصناعية وإمكانية استغلال هذا الوجود في لحظات الأزمات.

https://www.ic٣.gov/CSA/٢٦.٤.٧/٢.٢٦.pdf

AP News

الصراع بين إيران وإسرائيل ودور الهجمات السيبرانية البارز والتقنيات الرقمية في مجريات المواجهة

في ٢٩ مارس ٢٠٢٦، نشرت وكالة أسوشيتد برس تقريراً بقلم ديفيد كلير بعنوان: «اختراق المستشفيات وبرمجيات التجسس الخفية: الحرب الإيرانية تُظهر كيف أصبح القتال الرقمي جزءاً من الحروب الحديثة». تركز الرواية الرئيسية للتقرير على أن الحرب بين إيران وإسرائيل وحلفائهما الغربيين لم تعد حرباً عسكرية تقليدية، بل تحولت إلى حرب هجينة تتداخل فيها الهجمات السيبرانية وبرمجيات التجسس والمعلومات المضللة والذكاء الاصطناعي كعناصر

أساسية. في بداية التقرير، يوضح الكاتب مثالاً محدداً: خلال الهجمات الصاروخية الإيرانية على إسرائيل، تلقى بعض المواطنين الإسرائيليين رسائل نصية تبدو وكأنها توجههم إلى تطبيقات للعثور على الملاجئ الآمنة. لكن هذه الروابط كانت في الواقع برمجيات خبيثة، وعند تثبيتها كانت تتيح للمهاجمين الوصول الكامل إلى الكاميرا والموقع الجغرافي وبيانات الهاتف. وتشير الرواية إلى أن هذه العمليات نُسبت إلى إيران، وتُظهر مستوى التنسيق بين الهجمات السيبرانية والهجمات العسكرية الفعلية. ويؤكد الكاتب أن هذا النوع من الهجمات يمثل نمطاً جديداً في الحروب الحديثة، حيث تُنفذ العمليات الرقمية بالتزامن مع الضربات العسكرية بهدف إحداث أقصى تأثير نفسي وتشغيلي. ووفقاً لخبراء الأمن السيبراني الذين نقل عنهم التقرير، فإن هذا التزامن بين إطلاق الصواريخ ونشر البرمجيات الخبيثة غير مسبوق، ويشير إلى أن الحرب السيبرانية أصبحت جزءاً لا يتجزأ من ساحة القتال. ويذكر التقرير أن مجموعات قرصنة مرتبطة بإيران نفذت مئات العمليات السيبرانية ضد أهداف في الولايات المتحدة وإسرائيل ودول المنطقة. ورغم أن كثيراً من هذه الهجمات لا تسبب أضراراً تقنية واسعة، فإن هدفها الأساسي هو الضغط النفسي، وإثارة عدم الثقة، وإحداث اضطراب في الأنظمة الأضعف. وغالباً ما تستهدف هذه الهجمات مؤسسات ذات أمن سيبراني ضعيف أو بنى تحتية قديمة. ومن المحاور الرئيسية أيضاً استهداف القطاعات الحيوية مثل المستشفيات ومراكز البيانات وشركات التكنولوجيا الطبية والبنية التحتية العامة. ويشير التقرير إلى أن بعض الهجمات اخترقت بالفعل أنظمة مستشفيات وشركات معدات طبية في الولايات المتحدة، وفي بعض الحالات أدت إلى تعطيل الشبكات الداخلية. وتوضح الرواية أن الهدف الأساسي لهذه الهجمات هو خلق الفوضى والاضطراب أكثر من تحقيق مكاسب مالية. وفي جزء آخر، يناقش التقرير دور الذكاء الاصطناعي، موضحاً أنه ساهم في تسريع وتوسيع نطاق الهجمات السيبرانية، كما جعل إنتاج المعلومات المضللة (مثل التزييف العميق – deepfakes) أكثر سهولة. ونتيجة لذلك، أصبح الفضاء المعلوماتي مشوشاً للغاية، وأصبح من الصعب على الجمهور التمييز بين الحقيقة والزيف. وقد انتشرت أمثلة مثل مقاطع فيديو مزيفة لهجمات على سفن أمريكية أو لقطات مفبركة من ساحات القتال على نطاق واسع عبر وسائل التواصل الاجتماعي. وفي الخلاصة، يرى الكاتب أن الحرب بين إيران وحلفائها من جهة، وإسرائيل والولايات المتحدة من جهة أخرى، دخلت مرحلة أصبح فيها الفضاء الرقمي وساحة القتال الفعلية متداخلين بشكل كامل. وفي هذا السياق، لم تعد الهجمات السيبرانية أداة ثانوية، بل أصبحت جزءاً أساسياً من الاستراتيجية العسكرية والسياسية للدول. ويختتم التقرير بالإشارة إلى أن هذا النوع من الحرب سيستمر حتى في حال وقف إطلاق النار، لأنه أسرع وأقل تكلفة سياسياً من الحرب التقليدية، ويهدف أساساً إلى التجسس والتخريب وبث الخوف وتقويض الثقة بدلاً من الاحتلال العسكري.

https://apnews.com/article/iran-us-war-israel-data-centers-hacking-

CNBC

هددت إيران شركات التكنولوجيا الكبرى مثل إنفيديا وآبل وغيرها من عمالقة التكنولوجيا بشنّ هجمات

في ١ أبريل ٢٠٢٦، نُشر تقرير في قسم التكنولوجيا لدى CNBC بقلم كاي نيكول-شوارز، وتتمثل الرواية الرئيسية للكاتبة في أن الحرب بين إيران والولايات المتحدة/إسرائيل تجاوزت مستوى الصراع العسكري التقليدي لتصل إلى مجالات الاقتصاد الرقمي والبنية التحتية التقنية العالمية. وفقاً للتقرير، قامت إيران عبر الحرس الثوري الإيراني بتحديد شركات التكنولوجيا الأمريكية الكبرى كأهداف مشروعة وهددت بشن هجمات مباشرة عليها. وتوضح الرواية أن شركات مثل Nvidia وApple وMicrosoft وGoogle لم تعد مجرد كيانات اقتصادية، بل أصبحت جزءاً من ساحة

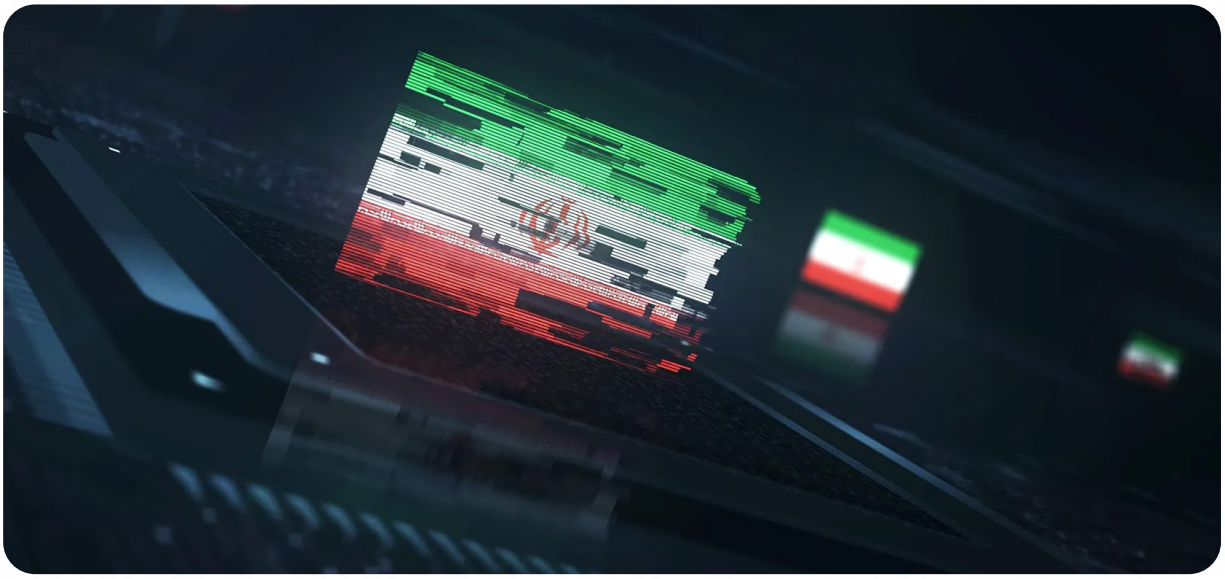
الحرب. وفي بيان منسوب إلى الحرس الثوري، تم الإعلان عن أن أي شركة أمريكية يمكن أن تصبح هدفاً رداً على عمليات الاغتيال والهجمات، مع إصدار تحذيرات تدعو موظفي هذه الشركات إلى مغادرة أماكن العمل لتجنب المخاطر المحتملة. ويشير التقرير أيضاً إلى قائمة تضم نحو ١٨ شركة تكنولوجيا وبنية تحتية، من بينها Cisco وIntel وOracle وIBM وDell وPalantir وJPMorgan وTesla. وتؤكد الرواية أن هذه التهديدات ليست مجرد رسائل سياسية أو دعائية، بل تعكس نمطاً جديداً في الحرب، حيث أصبحت البنى التحتية الرقمية ومراكز البيانات والخدمات السحابية أهدافاً عسكرية محتملة. وفي جزء آخر، ينقل التقرير عن خبراء في الأمن السيبراني، من بينهم الرئيس التنفيذي لشركة Healix، أن هذا التحول ليس مؤقتاً، بل يمثل تغييراً بنيوياً في طبيعة الحروب الحديثة. فوفقاً للرواية، أصبحت التكنولوجيا والأصول الرقمية لا تقل أهمية عن الأهداف العسكرية التقليدية، بل إن مراكز البيانات والبنية السحابية قد تصبح مستقبلاً أهدافاً تعادل القواعد العسكرية. كما يذكر التقرير أن بعض الهجمات السيبرانية السابقة المنسوبة إلى مجموعات مرتبطة بإيران تسببت في اضطرابات داخل مراكز بيانات تابعة لـ AWS في منطقة الشرق الأوسط، وأدت إلى تعطيل خدمات رقمية في دول مثل الإمارات. ويشير ذلك إلى أن الحرب السيبرانية أصبحت تؤثر بشكل مباشر على الحياة اليومية والخدمات الرقمية والاقتصاد الرقمي. وفي الخلاصة، ترى الكاتبة أن الحرب بين إيران والغرب دخلت مرحلة جديدة تلاشت فيها الحدود بين الحرب العسكرية والسيبرانية والاقتصادية. وفي هذا السياق، أصبحت شركات التكنولوجيا ومراكز البيانات والبنى التحتية الرقمية جزءاً من ساحة القتال، ما أدى إلى زيادة المخاطر العالمية، وعدم الاستقرار في سوق التكنولوجيا، وإعادة تعريف مفهوم الأمن القومي.

https://www.cnbc.com/٠١/٠٤/٢٠٢٦/iran-irgc-nvidia-appple-attack-threat.html

روداو

اختراق المستشفيات، وبرمجيات التجسس الخفية؛ الحرب الإيرانية تُظهر كيف تم دمج القتال الرقمي في الحرب الحديثة

في ٢٩ مارس ٢٠٢٦، نُشر تقرير مفصل لوكالة أسوشيتد برس بقلم ديفيد كلير بعنوان: «اختراق المستشفيات، وبرمجيات التجسس الخفية: الحرب الإيرانية تُظهر كيف تم دمج القتال الرقمي في الحرب الحديثة». تركز الرواية الرئيسية للكاتب على أن الحرب بين إيران والولايات المتحدة وإسرائيل لم تعد مجرد حرب عسكرية تقليدية، بل أصبحت مرتبطة بشكل عميق بالفضاء الرقمي والنفسي والمعلوماتي. ويشير التقرير إلى أنه بالتزامن مع الهجمات الصاروخية الإيرانية، نُفذت عملية سيبرانية معقدة ضد المواطنين



الإسرائيليين. فعلى سبيل المثال، تلقى بعض مستخدمي هواتف أندرويد أثناء توجههم إلى الملاجئ رسائل نصية تبدو وكأنها تقودهم إلى تطبيقات لمعرفة أماكن آمنة، لكن هذه الروابط كانت في الواقع برمجيات خبيثة تقوم بتثبيت برامج تجسس، وتتيح للمهاجمين الوصول إلى الكاميرا والموقع الجغرافي والبيانات الشخصية. وتوضح الرواية أن هذه الهجمات تعكس مستوى غير مسبوق من التنسيق بين العمليات العسكرية والهجمات الرقمية، حيث أصبح كل من «الخوف والمعلومات» سلاحين في ساحة الحرب الحديثة. ويذكر التقرير أن المجموعات المرتبطة بإيران لا تقتصر على الهجمات السيبرانية فقط، بل تستخدم أيضاً أدوات أوسع مثل المعلومات المضللة والذكاء الاصطناعي والعمليات النفسية. والهدف من هذه الأنشطة ليس فقط تدمير البنى التحتية، بل أيضاً خلق حالة من الارتباك وعدم الثقة والضغط النفسي على المجتمعات المستهدفة. وبحسب خبراء الأمن السيبراني الذين نقل عنهم التقرير، فإن حجم الهجمات كبير جداً، لكن الكثير منها لا يسبب أضراراً تقنية واسعة، إلا أنها تفرض ضغطاً كبيراً على المؤسسات الأمنية والشركات، وتجبرها على استهلاك موارد كبيرة للحماية ومعالجة الثغرات. كما تركز الرواية على أن الأهداف الرئيسية لهذه الهجمات تشمل البنى التحتية الحيوية مثل المستشفيات ومراكز البيانات وأنظمة النقل. وفي مثال آخر، أعلنت مجموعة قرصنة مرتبطة بإيران مسؤوليتها عن هجوم على شركة تكنولوجيا طبية في الولايات المتحدة، حيث تم تفعيل برمجية فدية عطّلت أنظمتها الداخلية. ويُلاحظ أن بعض هذه الهجمات لا تتضمن طلب فدية، بل تهدف فقط إلى إحداث فوضى وتعطيل. وفي جزء آخر، يناقش التقرير دور الذكاء الاصطناعي، موضحاً أنه ساهم في تسريع وتوسيع نطاق الهجمات السيبرانية، كما أصبح أداة رئيسية في الحرب المعلوماتية من خلال إنتاج صور مزيفة، وأخبار كاذبة، ومقاطع فيديو مزيفة (deepfakes). وقد وصلت بعض هذه المواد إلى مئات الملايين من المشاهدات، ما يجعلها مؤثرة بشكل كبير على الرأي العام. وفي الخلاصة، يرى الكاتب أن الحرب الإيرانية لم تعد محصورة في ساحة القتال التقليدية، بل تحولت إلى حرب هجينة رقمية-مادية، حيث أصبحت الهجمات السيبرانية وبرمجيات التجسس والعمليات النفسية والذكاء الاصطناعي أدوات رئيسية للقوة. ويؤكد التقرير أن هذا النوع من الحروب أقل تكلفة من الحرب التقليدية، لكنه أكثر انتشاراً وتأثيراً واستمرارية، وقد يستمر حتى بعد توقف العمليات العسكرية.

https://www.axios.com/٣١/٠٣/٢٠٢٦/iran-fbi-leaks-lockheed-

World Economic Forum

كيف تعيد حرب الشرق الأوسط تشكيل المشهد العالمي للأمن السيبراني

في ٢٥ مارس ٢٠٢٦، نُشر تقرير بقلم سبنسر فينغولد، رئيس التحرير الرقمي للمنتدى الاقتصادي العالمي، بعنوان: «كيف تعيد حرب الشرق الأوسط تشكيل المشهد العالمي للأمن السيبراني»، وتم تحديثه في ١ أبريل ٢٠٢٦. وتتمثل الرواية الرئيسية للكاتب في أن الحرب الجارية في الشرق الأوسط ليست مجرد صراع إقليمي، بل أصبحت عاملاً يغيّر البنية الأساسية للأمن السيبراني العالمي، وأدى ذلك فعلياً إلى تلاشي الحدود بين الحرب التقليدية والحرب الرقمية. ويؤكد التقرير أن الهجمات السيبرانية واسعة النطاق تجري بالتزامن مع العمليات العسكرية، ولا تقتصر على دول المنطقة، بل تمتد لتستهدف شركات

وبنى تحتية حيوية حول العالم. ووفقاً للرواية، لم تعد الحرب الحديثة محصورة في ساحة المعركة، بل امتدت إلى الفضاء السيبراني وشبكات البيانات وسلاسل الإمداد العالمية. ويشير التقرير إلى أمثلة تشمل هجمات برمجيات خبيثة ضد شركات طبية، وهجمات على شركات الطاقة، إضافة إلى اضطرابات في أنظمة النقل والقطاع المالي. وفي هذا السياق، يوضح الكاتب أن طبيعة التهديدات السيبرانية تغيرت من هجمات عشوائية أو انتهازية إلى عمليات موجهة ذات طابع جيوسياسي. وتوضح الرواية أن الفاعلين الدوليين والمجموعات الوكيلة أصبحوا يعملون بشكل منسق باستخدام أدوات مثل هجمات حجب الخدمة (DDoS)، وسرقة البيانات، وعمليات «الاختراق والتسريب» لتحقيق أهداف سياسية وعسكرية. ويؤكد التقرير أن الحدود بين الحرب السيبرانية والحرب المعلوماتية والحرب العسكرية أصبحت شبه غير موجودة. وفي جزء آخر، يسلط التقرير الضوء على البنية التحتية العالمية مثل الكابلات البحرية ومراكز البيانات، موضحاً أن التوترات الإقليمية يمكن أن تؤثر عليها بشكل مباشر، مما يؤدي إلى تباطؤ الاتصالات، وتعطيل الخدمات المالية، وخلق نقاط ضعف في الاقتصاد الرقمي العالمي. كما يناقش التقرير دور الذكاء الاصطناعي، مشيراً إلى استخدامه في أتمتة الهجمات السيبرانية وتسريع عمليات الاختراق، إضافة إلى إنتاج المعلومات المضللة ومقاطع الفيديو المزيفة (deepfakes). وقد أدى ذلك إلى تراجع الثقة في المعلومات الرقمية وزيادة عدم الاستقرار في الفضاء المعلوماتي. وتتمثل الفكرة الأساسية هنا في أن «حرب الحقيقة» أصبحت جزءاً من الصراع. وفي الخلاصة، يرى التقرير أن هذه التطورات تعكس دخول العالم مرحلة جديدة من «الحرب الهجينة»، حيث تتداخل الهجمات السيبرانية والعمليات النفسية والضغوط الاقتصادية والعمليات العسكرية بشكل متزامن. ويؤكد الكاتب أن أي دولة أو مؤسسة، حتى خارج مناطق النزاع، ليست بمنأى عن آثار هذه الحرب. ويخلص التقرير إلى أن حرب الشرق الأوسط تمثل إنذاراً عالمياً في مجال الأمن السيبراني، ما دفع الدول والشركات إلى إعادة صياغة استراتيجياتها الأمنية، مع التركيز على تعزيز المرونة الرقمية، وتقوية التعاون الدولي، وحماية البنى التحتية الحيوية من الهجمات المعقدة والمنسقة.

https://www.weforum.org/stories/٠٣/٢٠٢٦/middle-east-conflict-

Wired

ارتفاع الهجمات السيبرانية في الإمارات إلى ٥٣٠ ألف حالة يومياً بالتزامن مع الحرب الإيرانية

في تقرير نشرته WIRED Middle East، يُذكر أنه بالتزامن مع تصاعد التوترات العسكرية في الشرق الأوسط، واجهت دولة الإمارات العربية المتحدة موجة غير مسبوقة من الهجمات السيبرانية. وتتمثل الرواية الرئيسية للكاتب في أن الحرب الإيرانية لا تجري فقط في ساحة القتال التقليدية، بل هناك أيضاً حرب رقمية واسعة النطاق تدور في الخلفية وتستهدف البنية التحتية الحيوية للدول. ويشير التقرير إلى أن رئيس الأمن السيبراني في حكومة الإمارات أعلن أن

عدد الهجمات السيبرانية على البلاد وصل إلى نحو ٥٣٠ ألف هجمة يومياً، مقارنة بحوالي ٢٧٠ ألف هجمة قبل تصاعد التوترات. وتوضح الرواية أن هذا الارتفاع يعكس ارتباطاً مباشراً بين التطورات الجيوسياسية وتصاعد الضغط الرقمي خلال فترات الحرب. ويضيف التقرير أن هذه الهجمات تشمل محاولات اختراق، وهجمات حجب الخدمة (DDoS)، ومسحاً آلياً للشبكات، ومحاولات اختراق مستمرة للبنى التحتية الرقمية. ووفقاً للكاتب، فإن الهدف لا يقتصر على التدمير الفوري، بل يشمل أيضاً فرض ضغط دائم على أنظمة حساسة مثل القطاع المالي والطاقة والخدمات الحكومية. وتؤكد الرواية أن البنية التحتية الرقمية أصبحت ساحة حرب لا تقل أهمية عن البنية التحتية العسكرية التقليدية. وفي جزء آخر من التقرير، يُذكر أن بعض الهجمات المرتبطة بمجموعات يُعتقد أنها مرتبطة بإيران استهدفت أيضاً البنية السحابية مثل مراكز بيانات AWS ومنشآت نفطية، مما أدى إلى اضطرابات في الخدمات الرقمية وتوقف مؤقت لبعض عمليات الطاقة. ويشدد الكاتب على أن الهدف لم يعد مجرد سرقة بيانات، بل تعطيل العمليات على نطاق واسع. كما يناقش التقرير تحول طبيعة الهجمات السيبرانية، حيث بات المهاجمون يستخدمون أساليب أكثر تقدماً تشمل الاختراق الأولي، والبقاء داخل الأنظمة لفترات طويلة، ثم تفعيل الهجوم في «اللحظة صفر»، أي تعطيل البنى التحتية بشكل متزامن. ويشير هذا إلى انتقال الهجمات من نمط عشوائي إلى نمط استراتيجي منظم. وفي سياق آخر، يبرز التقرير دور الذكاء الاصطناعي، حيث تؤكد الجهات الأمنية في الإمارات أن العديد من هذه الهجمات أصبحت مؤتمتة بالكامل، بدءاً من رسائل التصيّد وصولاً إلى اختراق الشبكات والتحرك داخل الأنظمة. ويؤدي ذلك إلى تنفيذ دورة الهجوم دون تدخل بشري مباشر، مما يزيد من مستوى التهديد بشكل كبير. كما يشير التقرير إلى أن الحرب السيبرانية لم تعد مقتصرة على الحكومات والشركات، بل امتدت إلى الأفراد أيضاً، من خلال عمليات احتيال رقمية تستغل اضطرابات السفر والنقل، حيث ينتحل المهاجمون صفة شركات الطيران لسرقة البيانات أو الأموال. وفي الخلاصة، يرى التقرير أن الحرب الإيرانية والتوترات الإقليمية أدت إلى دخول الفضاء السيبراني مرحلة جديدة تتسم بزيادة السرعة والنطاق والأتمتة. وعلى الرغم من نجاح أنظمة الإمارات في احتواء جزء كبير من هذه الهجمات، فإن الاتجاه العام يشير إلى تصاعد مستمر في الشدة والتعقيد، مع تلاشي الحدود بين الحرب الرقمية والحرب التقليدية بشكل كامل.

https://www.wired.me/story/uae-cyberattacks-surge-to-٥٣٠...-per-day-

Foreign Policy

إيران تستعرض قدراتها السيبرانية

في ٣١ مارس ٢٠٢٦، نشر ريشي إيانغار تقريراً في مجلة Foreign Policy بعنوان: «إيران تستعرض قدراتها السيبرانية». وتتمثل الرواية الرئيسية للكاتب في أن التصعيد العسكري بين إيران والولايات المتحدة وإسرائيل ترافق مع تنشيط متزامن للجبهة السيبرانية، حيث تستخدم إيران قدراتها في الاختراق الإلكتروني كأداة رئيسية للردع والانتقام. في بداية التقرير، يشير الكاتب إلى هجوم سيبراني مثير للجدل نفذته مجموعة القرصنة "Handala Hack Team"، التي يُنسب ارتباطها بوزارة الاستخبارات الإيرانية، وتمكنت من الوصول إلى البريد الإلكتروني الشخصي القديم لرئيس مكتب التحقيقات الفيدرالي (FBI) كاش باتيل ونشر محتوياته، بما في ذلك صور شخصية ووثائق قديمة. وتوضح الرواية أن الهدف من هذه العمليات لا يقتصر على الحصول على البيانات، بل يتعداه إلى إحداث تأثير إعلامي ونفسي واسع. ويؤكد التقرير أن هذه الهجمات تأتي ضمن دورة متبادلة من

«الهجوم والرد» بين إيران من جهة، والولايات المتحدة وإسرائيل من جهة أخرى. وخلال هذه الفترة، قامت وزارة العدل الأمريكية بمصادرة مواقع إلكترونية مرتبطة بمجموعات قرصنة إيرانية، في حين نفذت هذه المجموعات هجمات على شركات أمريكية، خصوصاً في القطاعين الطبي والدفاعي. ومن أبرز الأمثلة الهجوم على شركة المعدات الطبية Stryker الذي أدى إلى تعطيل أنظمتها التشغيلية. وتشير الرواية إلى أن المجموعات السيبرانية الإيرانية تسعى في الوقت نفسه إلى تحقيق ثلاثة أهداف: تدمير البنية التحتية، وتسريب المعلومات الحساسة، وخلق ضغط نفسي على الخصوم. كما تدّعي بعض هذه المجموعات أنها سرقت كميات كبيرة من البيانات من شركات دفاعية مثل لوكهيد مارتن، رغم أن هذه الادعاءات لم يتم تأكيدها رسمياً. ومع ذلك، يشدد التقرير على أن الغموض والمبالغة جزء من استراتيجية هذه المجموعات. وفي القسم التحليلي، يوضح خبراء الأمن السيبراني أن هذه العمليات تمثل مزيجاً من الحقائق والمعلومات المضللة، بهدف إرباك الخصم وزيادة تكاليف الدفاع. ويصف أحد الخبراء هذا النوع من النشاط بأنه «حملات دعائية سيبرانية»، حيث يتم دمج الهجوم التقني مع بناء الرواية الإعلامية في وقت واحد. كما يشير التقرير إلى تغير طبيعة المجموعات السيبرانية المرتبطة بإيران، حيث تتلاشى الفوارق بين القراصنة المدعومين من الدولة والمجرمين الإلكترونيين. وتستخدم بعض هذه المجموعات نماذج اقتصادية جديدة تتيح للمهاجمين الحصول على حصة من الأرباح مقابل استهداف «أعداء إيران»، ما يعكس تداخل الدوافع المالية والسياسية والأيديولوجية. وفي جزء آخر، يقارن التقرير بين النهج الإيراني والروسي في استخدام برمجيات الفدية، موضحاً أن المجموعات الروسية تميل إلى تحقيق مكاسب مالية، بينما تركز المجموعات المرتبطة بإيران على التخريب وإحداث الاضطراب أكثر من الربح المالي. وبالتالي، فإن الهدف الأساسي لإيران في الفضاء السيبراني هو الردع وإيقاع الضرر وليس الكسب الاقتصادي. وفي الخلاصة، يؤكد التقرير أن إيران تستخدم الفضاء السيبراني كأداة رئيسية في الرد على الهجمات العسكرية، وأن هذه الأنشطة لا تقتصر على فترة الحرب فقط. فحتى في حال التوصل إلى هدنة، يتوقع الخبراء استمرار الهجمات السيبرانية نظراً لطبيعتها منخفضة التكلفة، وصعوبة تتبعها، وإمكانية إنكارها. وتخلص الرواية إلى أن إيران أنشأت عبر الحرب السيبرانية جبهة دائمة ومستمرة إلى جانب الحرب التقليدية، حيث لا يقتصر الهدف على التدمير، بل يشمل أيضاً استعراض القوة، وبث الخوف، واستنزاف الخصوم نفسياً وتقنياً.

https://foreignpolicy.com/٣١/٠٣/٢٠٢٦/iran-war-cyber-attack-hacking-kash-

خلاصة وتحليل خبير:

في الخلاصة، يمكن القول إن ما يتضح من التقارير والتحليلات الواردة في هذا المجلة هو إعادة تعريف لطبيعة الحرب في العصر الحديث؛ حرب لم تعد تُفهم فقط ضمن ساحات القتال التقليدية، بل أصبحت شبكة متعددة الطبقات وعابرة للحدود، تدور في مجالات سيبرانية، معلوماتية، اقتصادية ونفسية في آن واحد. وتشير تجربة الحرب الإيرانية وما رافقها من تداعيات سيبرانية إلى أن الحدود بين «السلام» و«الصراع» أصبحت أكثر ضبابية، وأن الأعمال العدائية يمكن أن تتجسد في هجمات رقمية غير مرئية تُحدث آثاراً تعادل أو تفوق أحياناً تأثير النزاعات العسكرية المباشرة. ومن أهم النتائج التي يبرزها هذا التحليل أن البنى التحتية الحيوية للدول أصبحت محوراً رئيسياً في التنافس الجيوسياسي. فالهجمات المتكررة على قطاعات مثل الطاقة، المياه، النقل، الصحة والشبكات الصناعية لا تهدف فقط إلى إحداث تعطيل مؤقت، بل إلى تقويض ثقة الجمهور، وزيادة كلفة الحوكمة، وفرض ضغط مستمر على الحكومات. وفي هذا السياق، تصبح نقاط الضعف البنيوية الناتجة عن الاعتماد على الشبكات المتصلة، وتقادم الأنظمة التقنية، وتعقيد سلاسل التوريد، عوامل أساسية في تصعيد التهديدات السيبرانية. ومن جهة أخرى، يؤكد هذا الطرح على الترابط الوثيق بين الحرب السيبرانية والحرب التقليدية. فالأدلة تشير إلى أن العمليات الرقمية لا تقتصر على كونها مكمّلة للعمليات العسكرية، بل غالباً ما تكون مقدمة لها أو متزامنة معها أو امتداداً لها. ويشمل ذلك استخدام البرمجيات الخبيثة، وبرامج التجسس، وهجمات حجب الخدمة، والتسلل إلى الاتصالات الشخصية والمؤسساتية، بهدف تحقيق تفوق معلوماتي وإضعاف قدرة الخصم على اتخاذ القرار. وهذا يعكس اتجاهاً واضحاً نحو «دمج ميادين الحرب» في الصراعات المعاصرة. ومن النقاط المهمة أيضاً دور «حرب الروايات» في الفضاء السيبراني. ففي عالم يتم فيه تداول البيانات والمعلومات والادعاءات بسرعة كبيرة، تتلاشى الحدود بين الحقيقة والدعاية السياسية. وينتج عن ذلك بيئة من الغموض الاستراتيجي، حيث يمكن حتى للأحداث التقنية أن تحمل أبعاداً سياسية وإعلامية. وهذا بدوره يزيد من صعوبة اتخاذ القرار لدى الدول، ويتيح للفاعلين المختلفين استخدام هذا الغموض كأداة ضغط. وأخيراً، فإن دخول تقنيات مثل الذكاء الاصطناعي إلى مجال العمليات السيبرانية أضاف مستوى جديداً من التعقيد. فالأتمتة في تنفيذ الهجمات، وزيادة سرعة الاستجابة، وإنتاج المحتوى المزيف، وتنفيذ عمليات واسعة النطاق، كلها مؤشرات على أن مستقبل التهديدات السيبرانية يتجه نحو مزيد من الذكاء والديناميكية. وبناءً على ذلك، يمكن الاستنتاج أن مواجهة هذا النوع من الحروب تتطلب إعادة نظر جذرية في مفاهيم الأمن القومي، وتعزيز صمود البنية التحتية، ورفع مستوى الوعي السيبراني، وتطوير التعاون الدولي. وإلا فإن الدول ستجد نفسها أمام تهديدات لا تعترف بالحدود، وتبقى حاضرة بشكل دائم وغير مرئي داخل البنى الحيوية لاقتصاداتها ومجتمعاتها.

حولنا:

مركز دراسات الشهيد الخامس هو مؤسسة بحثية مستقلة تركز على تحليل قضايا العراق والمنطقة في مجالات السياسة الداخلية والخارجية، والاقتصاد، والثقافة. يعتمد المركز على فريق من الخبراء والباحثين المتمرسين لدراسة الأوضاع الداخلية والخارجية في العراق، بهدف توفير منصة لتحليل عميق وشامل لدور العراق في المعادلات الإقليمية والدولية. يسعى المركز، من خلال الأبحاث الأكاديمية، والمقالات التحليلية، والجلسات التخصصية، إلى تعزيز فهم أفضل للاتجاهات المختلفة داخل العراق، ويهدف إلى تقديم رؤى استراتيجية تسهم في تحقيق التنمية المستدامة في البلاد.