الدروس التي يمكن لإسرائيل استخلاصها من الهجمات السيبرانية على أوكرانيا

بواسطة أوفير بارل (/ar/experts/awfyr-barl)

سبتمبر
متوفر أيضًا باللغات:
English (/policy-analysis/what-cyber-attacks-against-ukraine-can-teach-israel)

عن المؤلفين

أوفير بارل (/ar/experts/awfyr-barl)

أوفير بارل باحث في ورشة يوفال نئمان للعلوم والتكنولوجيا والأمن في جامعة تل أبيب وهو أيضًا باحث سابق في معهد دراسات الأمن القومي الإسرائيلي وفي مركز البحث السياسي في وزارة الخارجية الإسرائيلية بارل هو مساهم في منتدى فكرة

تحليل موجز

ينبغي على إسرائيل النظر إلى الحرب في أوكرانيا للحصول على نظرة ثاقبة للهجمات السيبرانية المتوقعة والاستراتيجيات الأمنية قبل الانتخابات التشريعية المقرر عقدها في تشرين الثاني/نوفمبر

يتعامل الناخبون المحليون مع الانتخابات المرتقبة للكنيست الخامس والعشرين في إسرائيل بلامبالاة وتشاؤم إذ يتمثل الفكر السائد في البلاد في أن ما لم تحقّقه الحملات الانتخابية الأربع السابقة التي حصلت منذ عام 2019 أي القرار السياسي لن تحقّقه انتخابات الأول من تشرين الثاني/نوفمبر وتشير استطلاعات الرأي الحالية (https://www.jpost.com/israel-news/article-715640) إلى أن هذا التقدير قد يكون صحيحًا

إلا أن الانتخابات الجديدة تفتح المجال أيضًا أمام التهديدات في مجال الحرب السيبرانية وعمليات التأثير وقد برزت هذه التكتيكات في دولٍ أخرى ولكنها لم تحقق أثرًا في إسرائيل حتى الآن ويرجع ذلك الى انخفاض معدلات استخدام وسائل التواصل الاجتماعي بين اليهود الأرثوذكس المتشددين ومع ذلك فإن تصاعد الهجمات الإلكترونية ضد أوكرانيا هذا العام تشير إلى الاتجاه الذي تتخذه هذه الهجمات وتُظهر الأثر المدمّر الذي قد تتسببه تلك الهجمات في إسرائيل ما لم تتم معالجتها بالشكل المناسب

لقد شنت روسيا منذ شباط/فبراير 2022 سلسلةً من الهجمات السيبرانية وعمليات التأثير ضد دول الغرب وأوكرانيا مما يشير الى توسع نطاق عملياتها السيبرانية. واستنادا الى استراتيجيات روسيا هناك ثلاثة تكتيكات رئيسية للتدخل في الانتخابات التشريعية لعام 2022:

تتمثل الوسيلة الأولى في استخدام الوسائط المعدّة باستخدام التزييف العميق وهي عبارة عن صور ومقاطع فيديو (ونصوص في بعض الأحيان) مزيّفة ويتم إعدادها باستخدام الوسائل التكنولوجية القائمة على الذكاء الاصطناعي ويتمثل الهاجس الرئيسي في السياق العسكري أو السياسي في نشر الجهات الفاعلة الخبيثة فيديوهاتٍ مزيّفة يظهر فيها القادة وهم يدلون بتصاريح لم يتم الإدلاء بها وبالتالي التلاعب بالرأي العام

ففي منتصف شهر آذار/مارس على سبيل المثال تردد (https://techcrunch.com/2022/03/16/facebook-zelensky-deepfake/) أن جهاتٍ مناصرة لروسيا نشرت فيديو مزيّف يظهر فيه الرئيس الأوكراني فولودومير زيلينسكي وهو يدعو شعبه للاستسلام وبعد ثلاثة أشهر (https://www.theguardian.com/world/2022/jun/25/european-leaders-deepfake-video-calls-mayor-of-kyiv-vitali-klitschko) خرق رجلٌ انتحل هوية عمدة مدينة كييف فيتالي كليتشكو اتصالاً عبر الفيديو جمع رؤساء العواصم الأوروبية بعد أن نجح في التخفي باستخدام الذكاء الاصطناعي

وتجدر الإشارة إلى أن استخدام تكنولوجيا التزييف العميق ليس بالجديد وقد عززت القدرة المتزايدة على الوصول إلى الوسائل التكنولوجية وتحمّل تكلفتها نطاقَ استخدام هذه التكنولوجيا بشكلٍ ملحوظ. هذا وقد ازداد عدد الفيديوهات المزيّفة المنشورة عبر الإنترنت حيث تضاعف كل ستة أشهر تقريبًا بين عامَي 2018 و2020. إلا أن حادثة الفيديو المزيف لزيلينسكي شكّلت سابقةً في هذا المجال إذ أنه لم يتم تسجيل أي حالة استخدمت فيها دولةٌ أو أي جهة تعمل باسمها تكنولوجيا التزييف العميق لأغراض تحقيق التأثير السياسي أو العسكري في دولةٍ أخرى.

ويمكن لهذه السابقة نفسها التي جرى فيها تحويل التهديد النظري إلى حقيقة أن تدفع بالجهات المعادية لإسرائيل إلى تخريب المسار الصحيح للانتخابات من خلال نشر الفيديوهات المزيّفة. وحتى ولو كانت هذه الفيديوهات متدنية الجودة ولم تنجح في خداع عددٍ كبيرٍ من الناخبين لكنها قد تودي الى تفاقم انعدام الثقة في صفوف المواطنين. قد يلفت الاهتمام الكبير الذي من المتوقع أن يوليه الإعلام لها (تمامًا كما حصل في الحالتين المذكورتين أعلاه) انتباه الناخبين الإسرائيليين إلى ضعف النظام المحلي الذي يفتقر إلى الحلول لهذه التهديدات. وهذا أحد الأهداف البارزة لناشري المعلومات المزيّفة (https://theconversation.com/why-public-trust-in-elections-is-being-undermined-by-global-disinformation-campaigns-181825). وسيكون من السهل تحقيقه في هذه الحالة نظرًا للارتباك والانقسام السياسي المتزايد والدورات الانتخابية المتكررة منذ عام 2019.

وتقوم الوسيلة الثانية على الاستخدام المتزايد لروبوتات الإنترنت لأغراض نشر المعلومات الخاطئة. ولا يُعد استخدام روبوتات الإنترنت كوسيلةٍ لتحقيق التأثير السياسي ممارسة جديدة لذا يمكن القول بالاستناد إلى نتائج الأبحاث التي أُجريت في السنوات الأخيرة إنّ روبوتات الإنترنت قد تشكّل سلاحًا تلاعبيًا مهمًا من حيث عدد الرسائل التي تنشرها وقدرتها على التأثير في الخطاب السياسي في آن. ففي نيسان/أبريل 2018 نشر "مركز بيو للأبحاث" دراسةً (https://www.pewresearch.org/fact-tank/2018/04/09/5-things-to-know-about-bots-on-twitter/) نظرت في نشر نحو 380 ألف تغريدة لمدة ستة أسابيع شملت روابط إلى مواقع إلكترونية إخبارية. وتبيّن أن ثلثي التغريدات نشرتها روبوتات الإنترنت. بالإضافة إلى ذلك نشر "المكتب الوطني للبحوث الاقتصادية" دراسةً بعد شهرٍ واحد (https://www.nber.org/system/files/working_papers/w24631/w24631.pdf) أظهرت أنه خلال فترة الانتخابات الرئاسية الأمريكية لعام 2016 والاستفتاء البريطاني ساهمت روبوتات الإنترنت مساهمةً ملحوظة في تشكيل غرف الصدى وهي مساحات افتراضية يمكن استخدامها لترداد الرسائل الخاطئة وتعزيز نشر الرسائل الخلافية.

هذا ويتمثل الابتكار الذي شهدته الحرب في أوكرانيا في الاستخدام المتزايد لمزارع الروبوت التي تضم أعدادًا هائلة من روبوتات الإنترنت. فقد عمدت أوكرانيا إلى تعطيل ستّ مزارع في شهرَي آذار/مارس وآب/أغسطس (https://www.zdnet.com/article/ukraine-takes-out-five-bot-farms-spreading-panic-among-citizens/#ftag=RSSbaffb68) (https://bit.ly/3BRicFD) كانت تضم مجموع 1.1 مليون روبوت إنترنت أي ما يوازي نحو 183 ألف روبوت في المزرعة الواحدة. ولغرض توضيح حجم التهديد يتخطى هذا الرقم عدد روبوتات الإنترنت التي يُقال إنها كانت نشطةً على موقع "تويتر" خلال الانتخابات الأمريكية لعام 2016 (وبقارب 50 ألف روبوت (https://techcrunch.com/2018/01/19/twitter-updates-total-of-russia-linked-election-bots-to-50000/)) بواقع 22 مرة.

وتجدر الإشارة أيضًا إلى أن الساحة السياسية الإسرائيلية اليوم معتادةٌ على الانخراط الواسع النطاق لروبوتات الإنترنت. ففي منتصف شهر آب/أغسطس أفادت وسائل الإعلام الإسرائيلية بأن "جهاز الأمن العام الإسرائيلي" ("شين بيت") نجح في نزع 140 ألف روبوت إنترنت إيراني (https://www.unitedagainstnucleariran.com/proxies-partners/shin-bet-reportedly-fears-russian-iranian-interference-upcoming-israeli-election) كانت تحاول التأثير في انتخابات آذار/مارس 2021.على ما يبدو يمتلك كلا من جهاز الأمن العام الإسرائيل والهيئة الوطنية للأمن السيبراني الموارد والقدرات للكشف عن شبكات الروبوت الضخمة المحتملة والعمل على إغلاقها. ومع ذلك سيؤدي استخدام المزيد من الروبوتات إلى مضاعفة العبء على السلطات الإسرائيلية وستتمكن المزيد من الروبوتات من الإفلات من التتبع وتقوم بنشر رسائل تخريبية ومثيرة للجدل وبالتالي تقويض المجتمع الإسرائيلي الذي أصبح بالفعل أكثر تشرذمًا وتضاربًا أكثر من أي وقت مضى. وينطبق هذا الأثر بشكل خاص في حالة استخدام روبوتات الذكاء الاصطناعي والتي تعتبر أكثر تعقيدًا ويصعب تتبعها.

أما الوسيلة الثالثة فتتمثل في خرق وسائل إعلام متنوعة بهدف نشر المعلومات الخاطئة. ففي 12 تموز/يوليو نشر "جهاز الدولة لحماية الاتصالات والمعلومات الخاصة في أوكرانيا" (SSSCIP) تقريرًا (https://www.infosecurity-magazine.com/news/ukraine-)

cyber-agency-cyber-attack/) ورد فيه ان عدد الحوادث السيبرانية التي شملت استخدام الرموز الخبيثة خلال الربع الثاني من عام 2022 قد ارتفع بنسبة 38% بالمقارنة مع الربع الأول من العام نفسه. ويشير التقرير إلى أنه خلال الفترة نفسها تعرّض قطاع الإعلام والقطاع الحكومي المحلي للعدد الأكبر من الهجمات السيبرانية من القراصنة الروس. وشهدت هذه الجهات نوعين مختلفين من الهجمات السيبرانية خلال الحرب وهما تعطيل بثّ وسائل الإعلام (على غرار الهجمة المنفّذة في تموز/يوليو **https://therecord.media/ukrainian-radio-broadcaster-hacked-to-spread-fake-news-about-zelenskys-health/)** ونُشرت فيها معلومات خاطئة حول حالة زيلينسكي الصحية) والهجمات التشويهية **https://www.mandiant.com/resources/blog/information-operations-surrounding-ukraine)** التي نشر في خلالها القراصنة الروس رسائل تهدف إلى الحط من معنويات الشعب ومفاقمة الانقسامات وتعزيز الدعم لروسيا.

شكّلت الهجمات السيبرانية من النوعين المذكورين أعلاه حتى الآن جزءًا ضئيلًا من الحرب السيبرانية التي تشنها إيران ضد إسرائيل. ففي واقع الامر لا يميل ميزان القوى بين إسرائيل وإيران في مجال الفضاء الإلكتروني لصالح أي الطرفين. غالبا ما تكون إسرائيل أكثر استعدادًا لتلك التهديدات السيبرانية ولديها قدرات هجومية فائقة ولكن من جهة أخرى صارت العمليات المعلوماتية الإيرانية - على الرغم من سوء إدارتها - أكثر تعقيدًا وأفضل تمويلًا في السنوات الأخيرة مما يضمن استمرار التهديدات حتى بعد حجبها نهائيا.

وفي ما يتعلق بتعطيل المنصات الإعلامية فقد سُجّلت الهجمة الأخيرة في كانون الثاني/يناير 2022 عندما هاجم **https://www.haaretz.com/israel-news/2022-01-03/ty-article/jerusalem-post-maariv-hacked-on-anniversary-of-soleimani-assasination/0000017f-f663-d887-a7ff-fee7876e0000)** القراصنة الإيرانيون موقع "جيروزاليم بوست" وحساب صحيفة "معاريف" على موقع "تويتر" بمناسبة ذكرى اغتيال قاسم سليماني غير أن إيران نفت ضلوعها في هذا الهجوم. إضافة الى ذلك عملت إيران على اظهار قوتها السيبرانية حيث تدخلت في الحوار الدائر حول الانتخابات الأمريكية لعام 2020 بغية إثبات كفاءتهم السيبرانية حين تلقّى الناخبون من عدة ولايات خلال فترة الانتخابات الرئاسية الأمريكية رسائل بالبريد الإلكتروني يُزعم أنها من جماعة "براود بويز" الأمريكية من اليمين المتطرف تهدد الناخبين لعدم انتخاب الرئيس ترامب. وتبيّن **https://www.bloomberg.com/news/articles/2022-01-27/iranians-behind-proud-boys-ruse-pose-wider-threat-fbi-says)** أن هذه الرسائل الإلكترونية التي تضمّنت معلوماتٍ شخصية عن المتلقّين قد أُرسلت بالنيابة عن إيران. وتشير قدرة القراصنة على الحصول على عناوين البريد الإلكتروني وتضمين المعلومات الشخصية فيها إلى أن الإيرانيين قادرون على الجمع بين القدرات السيبرانية الهجومية وقدرات الحرب النفسية بهدف التأثير في الرأي العام لغاياتٍ سياسية. ومن المتوقع ان تقوم إيران بشن إيران المزيد من الهجمات ذات الأثر النفسي ضد إسرائيل في المستقبل القريب.

في حين أن توظيف الحرب الإلكترونية في الحرب في أوكرانيا حمل تهديدات جديدة للانتخابات في إسرائيل فإن الإجراءات التي اتخذتها اوكرانيا تدعوا الى تنفيذ حلول فعالة لمعالجة هذه التهديدات. وتجدر الإشارة في هذا الصدد نوعين من الحلول المتنوعة التي قامت أوكرانيا والدول الغربية بتنفيذهما منذ اندلاع الحرب السيبرانية والمعلوماتية.

يتمثل الحل الأول في تعميق التعاون الدولي الذي تعمل إسرائيل بالفعل على تحقيقه فمنذ عام 2019 اتخذت إسرائيل عدة خطوات لحماية انتخاباتها من التدخل الأجنبي منها على سبيل المثال إنشاء فريق متخصص بقيادة الهيئة الوطنية للأمن السيبراني. ومع ذلك اوصى بعض خبراء المخابرات في إسرائيل بإنشاء مؤسسات دولية لحماية الانتخابات الوطنية. وفى ما يتعلق بالحرب في أوكرانيا يبدو أن هذا التعاون يحمل قيمة كبيرة ففي جلسة استماعٍ انعقدت في مجلس النواب الأمريكي زعم **https://www.fedscoop.com/ukraine-crisis-demonstrates-cyber-concept-of-persistent-engagement/)** رئيس "قيادة الأمن الإلكتروني الأمريكية" الجنرال بول ناكاسون أن أوكرانيا تعاملت مع الهجمات السيبرانية الروسية بصورةٍ أفضل مما كان متوقعًا عشية الغزو الروسي ويعود الفضل (جزئيًا) للمساعدة الغربية المقدّمة لها في مجال الأمن السيبراني. ويمكن لإسرائيل أن تستفيد من هذا النوع من التعاون الدولي من خلال تلقي الاستخبارات حول التهديدات المحتملة على سبيل المثال أو تعطيل البنية التحتية المستخدمة لشنّ الهجمات السيبرانية وعمليات التأثير.

وبما ان طبيعة الإنترنت تشير إلى أن شن بضع هجمات سيبرانية يمكنها ان تنجح في اختراق أكثر أنظمة الأمن السيبراني قوة يتحتم على اسرائيل ان تعمل على تعزيز المهارات الرقمية لدى مواطنيها. وتوفّر أوكرانيا في هذا المجال أيضًا نموذجًا عن حلٍ ناجح إذ ينفّذ "مجلس الأبحاث والتبادل الدولي" (آيركس) برنامجًا لتعليم المهارات الرقمية في أوكرانيا منذ عام 2015 وقد أطلق عليه اسم "التعلّم من أجل الإدراك" (Learn to Discern – L2D). **https://www.npr.org/2019/03/22/705809811/students-in-ukraine-learn-how-to-spot-fake-stories-propaganda-and-hate-speech)** وفي أيار/مايو كشف المجلس عن استبيانٍ **https://www.irex.org/success-story/irex-information-literacy-l2d-methodology-proving-vital-during-war-ukraine)** أجراه وشمل معلّمين في المرحلتين المتوسطة والثانوية تلقّوا التدريب من "آيركس". وأظهر هذا الاستبيان أن 90% من المعلّمين

استخدموا المعرفة التي اكتسبوها في إطار هذه التدريبات من اجل مساعدة الأصدقاء والأقارب والزملاء على فهم البيئة المعلوماتية الافتراضية. وكان قد تبيّن في السابق (https://www.irex.org/sites/default/files/node/resource/evaluation-learn-to-discern-in-schools-ukraine.pdf) أن محتوى البرنامج ساعد الطلاب على تحسين مهاراتهم الرقمية وتحسين قدراتهم على تحديد المنشورات المزيفة بنسبةٍ 18 في المئة. وعلى الرغم من أن الفترة المتبقية حتى موعد حصول الانتخابات باتت قصيرةً جدًا بحيث يصعب تنفيذ مثل هذا البرنامج بالكامل يجدر الشروع بتنفيذه في أقرب وقت ممكن من أجل تقليص الفجوة في المهارات الرقمية لدى الشعب الإسرائيلي في أسرع وقت واعدادهم لمواجهة الهجمات السيبرانية وعمليات التأثير. ❖

موصى به

IN-DEPTH REPORTS

U.S. Counterterrorism Reimagined:

Tracking the Biden Administration's Effort to Reform How America Addresses Violent Extremism

/ /

◆

Matthew Levitt

(/policy-analysis/us-counterterrorism-reimagined-tracking-biden-administrations-effort-reform-how)

تحليل موجز

عمليات الاستيلاء الإيرانية تثير تساؤلات حول العمليات البحرية بالمركبات غير المأهولة

سبتمبر

◆

فرزين نديمي

(ar/policy-analysis/mlyat-alastyla-alayranyt-tthyr-tsawlat-hwl-almlyat-albhryt-balmrkbat-ghyr-almahwlt/)

ARTICLES & TESTIMONY

In Rejecting Iran Nuclear Deal, Israeli Rivals Are of One Mind

/ /

◆

Neri Zilber

(/policy-analysis/rejecting-iran-nuclear-deal-israeli-rivals-are-one-mind)

TOPICS

الديمقراطية والإصلاح (/ar/policy-analysis/aldymqratyt-walaslah)

الشؤون العسكرية والأمنية (/ar/policy-analysis/alshwwn-alskryt-walamnyt)

المناطق والبلدان

إسرائيل (/ar/policy-analysis/asrayyl)