ظهور المرتزقة في المجال السيبراني

بواسطة نيري زيلبر (/ar/experts/nyry-zylbr-0)

سبتمبر
متوفر أيضًا باللغات:
English (**/policy-analysis/rise-cyber-mercenaries**)

عن المؤلفين

نيري زيلبر (/ar/experts/nyry-zylbr-0)

نيري زيلبر هو صحفي ومحلل سياسي وثقافي متخصص في الشرق الأوسط وزميل مساعد في معهد واشنطن.

مقالات وشهادة

ظهرت الرسالة النصية الأولى على هاتف أحمد منصور عند الساعة 9:38 من صباح أحد أيام آب/أغسطس الحارة عام 2016. كانت الرسالة غامضة بعض الشيء وباللغة العربية وقد ورد فيها ما يلي: "أسرار جديدة عن تعذيب الإماراتيين في سجون الدولة" وتبعها رابط تشعبي. وقد بدا كل من الرقم والرسالة والرسالة المشابهة التي تلقاها في اليوم التالي غريبًا بالنسبة إلى منصور وهو ناشط معروف في مجال حقوق الإنسان في دولة الإمارات العربية المتحدة. فقاوم وامتنع عن النقر على الروابط.

بدلاً من ذلك أرسل منصور الملاحظات إلى معهد أبحاث "سيتيزن لاب" التابع لجامعة تورنتو والمتخصص في حقوق الإنسان وأمن الإنترنت. وبعد العمل بالاتجاه المعاكس وجد الباحثون أن الروابط التشعبية هي جزء من برنامج تجسس متطور تم تصميمه خصيصًا لاستهداف منصور. ولو نقر على الروابط لحوّل البرنامج هاتفه إلى "جاسوس رقمي في جيبه" يتتبع تحركاته ويراقب رسائله ويسيطر على كاميرته وميكروفونه بحسب ما جاء **(https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/)** لاحقًا في تقرير "سيتيزن لاب".

لكن الاكتشاف المهم في التقرير لم يكن التكنولوجيا المستخدمة بحد ذاتها إذ قامت وكالات الاستخبارات في الدول المتقدمة بتطوير برامج تجسس ونشرها حول العالم. فما برز هو أن معهد "سيتيزن لاب" قد تعقّب البرنامج واكتشف أنه يعود إلى شركة خاصة وهي "مجموعة إن أس أو" الإسرائيلية الغامضة. (يتكون الاسم من الأحرف الأولى من أسماء مؤسسي الشركة الثلاثة). وبطريقة ما تمكنت هذه الشركة الصغيرة نسبيًا من العثور على ثغرة في أجهزة آيفون الجوالة التي تُعتبر من بين أكثر الأجهزة الخليوية أمنًا في العالم وقد طورت برنامجًا لاستغلالها – وهي عملية مكلفة للغاية وتستغرق وقتًا طويلاً. وفي هذا السياق كتب **(https://www.lawfareblog.com/private-sector-attribution-cyber-attacks-growing-concern-us-government)** باحثو معهد "سيتيزن لاب" في تقريرهم: "لسنا على علم بأي حالة سابقة تم فيها اختراق نظام حماية أجهزة آيفون عن بُعد ليُستخدم كجزء من حملة هجومية موجّهة".

وتُعد إسرائيل رائدةً على المستوى العالمي في قطاع التكنولوجيا السيبرانية الخاص حيث تملك على الأقل 300 شركة تغطي كافة المجالات بدءًا من الأمن المصرفي وصولاً إلى الدفاع عن البنية التحتية الحيوية. ولكن في حين أن معظم هذه المؤسسات تهدف إلى حماية الشركات من الهجمات الإلكترونية استغل بعضها هذا الخط الرفيع الفاصل بين القدرات الإلكترونية الدفاعية وتلك الهجومية لتزويد العملاء بخدمات أكثر شرًا. ففي حالة منصور يُعتقد أن الإمارات العربية المتحدة قد استخدمت أدوات زوّدتها بها شركة "إن أس أو" لمراقبة أشهر المعارضين في البلاد. (ويقضي منصور الآن حكمًا بالسجن لمدة 10 سنوات بسبب نشره "معلومات كاذبة" على حساباته الخاصة عبر وسائل التواصل الاجتماعي). وفي هذا الإطار كتب الباحث في مجال السياسات في مؤسسة "راند" ساشا رومانوسكي العام الماضي أنّ "هذه الشركات تقوم بتطبيق تقنيات متطورة أو ربما أكثر تعقيدًا من وكالات الاستخبارات الأمريكية".

ولا تزال خصخصة هذه القدرة الهجومية في مراحلها الأولى، إلا أنها تثير مخاوف واسعة بشأن انتشار بعض الأدوات بالغة القوة وبشأن الطريقة التي تفقد بها الحكومات القدرة على احتكار استخدامها. فعندما تستخدم الأطراف الفاعلة في الدولة الأسلحة الإلكترونية يكون هناك على الأقل إمكانية التنظيم والمساءلة. ولكن عندما تكون الشركات الخاصة هي الفاعلة تصبح الأمور أكثر تعقيدًا. وفي هذا الصدد تمثّل إسرائيل حالة اختبار جيدة. فهي تقدّم إمدادات ثابتة من مشغلي الإنترنت ذوي الكفاءات العالية الذين يتعلمون المهارة هذه أثناء خدمتهم العسكرية في واحدة من نخبة وحدات الاستخبارات في البلاد - والوحدة 8200 هي الأشهَر بينها – وينتقلون بعد ذلك للعمل في الشركات الخاصة. وقال نداف زافرير وهو جنرال متقاعد وقائد سابق للوحدة 8200 إنّ الجنود الذين يقضون وقتًا في الخدمة لحماية إسرائيل من الهجمات الإلكترونية ينتهي بهم الحال في معرفة كيفية مهاجمة الطرف الآخر. وأضاف "من أجل سد الثغرة بين الدفاع والهجوم يجب أن يكون لديك عقلية المعتدي".

ولم تكن قضية منصور مسألةً منفردة. فوفقًا (**https://citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/**) لمعهد "سيتيزن لاب" تم استهداف نحو 175 شخصًا من قِبل برامج التجسس التي طورتها مجموعة "إن أس أو" منذ عام 2016 ومن بينهم ناشطون في مجال حقوق الإنسان ومعارضون. ويشار إلى أن شركات إسرائيلية أخرى توفّر منتجات مماثلة. وفي هذا الإطار قال نيمرود كوزلوفسكي وهو أستاذ مساعد في "جامعة تل أبيب" ومحامٍ متخصص في الأمن السيبراني: "ما من طريقة أخرى فمن أجل تأمين الدفاع للشبكة ينبغي تحديد نقاط الضعف". ثم أضاف: "لقد تم إنشاؤها بناءً على معرفة [إسرائيل] المتعمقة بمكامن الضعف والطرق الهجومية هذه. فنحن على دراية تامة بالأهداف".

فلنأخذ على سبيل المثال أشهر هذه الأهداف المزعومة أي الهجوم الذي نفذته الوحدة 8200 بالتعاون مع "وكالة الأمن القومي" الأمريكية في عامي 2009 و2010 على منشأة إيرانية لتخصيب اليورانيوم في نطنز. لقد تمكنت الوحدة من نشر فيروس حاسوبي - يطلق عليه اسم "ستوكسنت" – داخل المرفق على الرغم من وجود فجوة هوائية هناك أي أن المرفق كان منفصلًا عمليًا عن شبكة الإنترنت الواسعة. واستهدف الفيروس نظام التشغيل لأجهزة الطرد المركزي المستخدمة في تخصيب اليورانيوم ما أدى إلى جعلها تتحرك بوتيرة خارجة عن السيطرة وتكسّرها. وعلى ما يبدو تم اختراق نظام المراقبة أيضًا إذ لم يلاحظ الإيرانيون بدايةً الضرر الذي كان يحدث.

ولعله ليس من الصدفة أن الكثير من منتجات شركات الدفاع الإلكتروني الإسرائيلية يهدف إلى إحباط الهجمات التي تكون على نمط "ستوكسنت" والتي تهاجم البنية التحتية الحيوية. فتضم هذه الشركات شركة "أبيريو سيستمز" التي يرأسها ضابط مخابرات سابق يدعى ليران تانكمان والتي طورت منتجًا يكتشف التلاعب بالبيانات - "آلة الحقيقة" كما يسميها تانكمان - في قراءات المستشعِرات في المنشآت الصناعية.

وبالرغم من أن "ستوكسنت" فيروسًا قديمًا ولا يُعمل به الآن سوى كأداة تحليلية بات اليوم مصدر اهتمام الخبراء في هذا المجال وذلك لسبب وجيه: لقد كان هجومًا إلكترونيًا ناجحًا للغاية ضد جهة تابعة للدولة وقد تسبب بأضرار مادية فعلية. وفي هذا الصدد قال الخبير غابرييل أفنر وهو مستشار الأمن الرقمي في إسرائيل "إن عقدًا واحدًا من الزمن في التكنولوجيا هو دهر". ففي أيامنا هذه تتزايد الهجمات السيبرانية بحسب ما قال زافرير وهو القائد السابق للوحدة 8200 ويدير اليوم شركة "تيم 8" وهي شركة تجمع بين صندوق للمشاريع الرأسمالية وحاضن ومختبر للأفكار. أمّا التطور الذي يقلقه ويقلق وخبراء آخرين فهو انتشار إنترنت الأشياء.

وفي هذا الصدد قال الخبير بالمسائل المتصلة بالفضاء الإلكتروني في "جامعة هارفارد" بروس شناير: "لقد تحول كل شيء إلى حاسوب: الهاتف والثلاجة وجهاز الميكروويف والسيارة". وتكمن المشكلة في أن شبكة الإنترنت التي ظهرت في السبعينيات والثمانينيات من القرن الماضي قد صُمّمت من دون مراعاة المسألة الأمنية. لذلك يتسابق الجميع الآن إلى سدّ الثغرات في أنظمة المعلومات (مثل البرمجيات) وأنظمة التشغيل (مثل المنشآت الصناعية المادية) قديمة الطراز أو المكتوبة بشكل سيئ أو غير الآمنة. ثم أضاف شناير وهو أيضًا مؤلف كتاب "انقر هنا لقتل الجميع: الأمن والصمود في عالم شديد الاتصال: "الهجمات أصبحت أسرع وأسهل وأفضل".

فهل يعني ذلك أننا هالكون جميعًا الإجابة المختصرة هي لا – أو أقله ربما لا. فحتى الآن إذا وضعنا "ستوكسنت" جانبًا تُعد الهجمات الإلكترونية الأكثر نجاحًا هي تلك التي استهدفت أوكرانيا وإستونيا وتسببت في أضرار مادية واسعة النطاق. وعلى الرغم من أن هذه الهجمات التي استهدفت شبكات الطاقة والمؤسسات المالية والوزارات الحكومية قد تسببت بأضرار فادحة تم تحديدها ومعالجتها بسرعة نسبيًا. ولم يحصل أي من سيناريوهات "يوم القيامة" التي يرغب بعض الخبراء أو النقاد في التحذير منها - مثل سيطرة المتسللين على سلاح نووي أو طائرة تجارية أو برامج ضارة تتسبب في انهيار وول ستريت.

ويعود ذلك جزئيًا إلى أنه "سيتوفر دائمًا للمتسللين الذين ترعاهم الدولة الموارد التي يحتاجونها" بحسب تانكمان. "إنما المهم هنا هو إلى أي مدى يسبق القطاع العام [الجهات غير التابعة للدولة]. لن يكون هناك أي "سلاح نووي سيبراني" خلال سنة أو سنتين من اليوم

إذ تكمن المسالة في وتيرة التطور بين المهاجمين والمدافعين فعليك ان تعمل بدون توقف".

وإذا كان جزء من الخطر نابع من الخط الضبابي الذي يفصل بين الدفاع السيبراني والهجوم السيبراني يأتي جزء آخر من التمييز شبه المعدوم بين المجالين الالكترونيين العام والخاص ففي تموز/يوليو على سبيل المثال أصدرت السلطات الإسرائيلية لوائح اتهام عدة ضد موظف سابق في مجموعة "إن أس أو" ادّعت فيها أنه سرق معلومات حساسة ومسجّلة الملكية وهو في طور مغادرته الشركة غير أن الموظف الذي لم يُكشف عن اسمه اتُهم أيضًا بمحاولة تقويض الأمن القومي: فقد حاول على ما يبدو بيع المعلومات بمبلغ قدره 50 مليون دولار أمريكي في عملة مشفرة إلى مشترٍ أجنبي على الشبكة المظلمة وهي جزء شاسع من الانترنت وغير ظاهر يتعذر الوصول إليه من خلال محركات البحث العادية

ولا تشكّل هذه الحادثة التي كشفتها الشركة بسرعة إلا حالة واحدة من بين العديد من الحالات التي توضح مدى ارتباط المجالين الخاص والعام في الحرب السيبرانية فالقدرات التي كانت تخص الحكومات وحدها تجد اليوم طريقها إلى الشركات خاصة التي غالبًا ما تكون مجرمة

وأصبحت شيفرة فيروس "ستوكسنت" متاحةً للعلن الآن ففي عام 2013 سرق متسللون – يُعتقد أنهم من الجنسية الروسية - سلاحًا إلكترونيًا طورته "وكالة الأمن القومي" مستغلةً نقاط الضعف في "مايكروسوفت ويندوز" ونشروه على الانترنت وفي أيار/مايو 2017 استخدم متسللون آخرون - ربما من كوريا الشمالية – هذا السلاح لإطلاق هجوم فيروس الفدية على صعيد العالم ويُعتقد أن الهجوم الذي حمل اسم "واناكراي" قد أصاب 200 ألف حاسوب في أكثر من 150 دولة ومنها أجزاء رئيسية من "دائرة خدمة الصحة الوطنية البريطانية" قبل أن يتم إيقافه وفي قضية منفصلة في عام 2013 أثبتت **(https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/)** **(https://www.reuters.com/article/net-us-hackers-virus-china-mandiant/mandiant-goes-viral-after-china-hacking-report-idUSBRE91M02P20130223)** شركة "مانديانت" وهي شركة خاصة للأمن السيبراني في الولايات المتحدة أن المتسللين الذين يعملون لصالح الجيش الصيني يستهدفون الشركات الأمريكية والوكالات الحكومية وفي عام 2015 قامت وحدة 8200 بحسب التقارير باختراق **(https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html)** شركة "كاسبرسكاي لاب" الرائدة عالميًا في برامج مكافحة الفيروسات كما اكتشفت أن الشركة الخاصة كانت تعمل كبوابة خلفية للمخابرات الروسية إلى عملائها ومن بينهم أكثر من وكالة حكومية أمريكية

وفي هذا السياق قال جنرال إسرائيلي متقاعد ومؤسس شركة "بلو أوشين تكنولوجيز" المتخصصة بالهجمات الالكترونية رامي بن أفرايم: "في العالم المادي للحروب لطالما عُرف بوضوح ما هو عام: أي الدبابات والقبة الحديدية (أنظمة الدفاع الصاروخي) وطائرات أف- . وتابع: "أمّا في العالم السيبراني اليوم فالأمر معقد" إذ يمكن أن تكون البنى التحتية الحيوية مثل مرافق الطاقة أو محطات معالجة المياه مملوكةً للقطاع الخاص كما هو غالبًا الحال في الولايات المتحدة ولكنها قد تتسبب في أضرار تطال البلد بأكمله إذا ما تعطلت أنظمتها وكذلك تمرّ رسائل تعبئة قوات الاحتياط الإسرائيلية في أوقات الحرب عبر شبكات الاتصالات الخاصة كما أن إنترنت الأشياء - التي ربطت الكثير من منتجاتنا الاستهلاكية - قد خلقت أيضًا نقاط ضعف هائلة

وأضاف بن أفرايم وهو طيار حربي سابق: "إذا كنت ترغب في إنزال طائرة وإذا كنت ترغب في الحصول على قوة جوية فأنت لا تدخل من الباب الأمامي أي قمرة القيادة بل تنال من المطار والأنظمة اللوجستية وتذهب خلف أجهزة الآيباد التي يأخذها معهم الطيارون إلى منازلهم". وأضاف بن أفرايم لم يعد هناك "كيانات قائمة بذاتها –فكلّ شيء أصبح جزءًا من شبكة". وحسبما أخبرني نائب وزير الدفاع في ليتوانيا إدفيناس كيرزا في الخريف الماضي في العاصمة فيلنيوس في إشارة إلى الإجراءات الروسية ضد الدول السوفيتية السابقة الأخرى: "إن الهجمات تأتي من الداخل – المصارف في تراجع والحكومة غير مستجيبة وهناك حالة عدم استقرار عام"لا فرق إن تم تحصين الحدود" كما يقولون "فنحن سنأتي من الداخل".

قد اختارت إسرائيل على سبيل المثال مكافحة المشكلة على مستوى الدولة عن طريق ربط المجالين العام والخاص وأحيانًا بكل ما للكلمة من معنى فمركز البلاد للفضاء السيبراني في مدينة بئر السبع الجنوبية لا يضم حرم التكنولوجيا الجديد التابع للجيش الإسرائيلي فحسب بل أيضًا مجمع شركات ذات تقنيات عالية ومركز النقب للأبحاث السيبرانية التابع لـ "جامعة بن غوريون" و"المديرية السيبرانية الوطنية" التي تتبع مباشرةً مكتب رئيس الوزراء وقال المستشار الأمني أفنير بإصرار: "هناك جسر مادي بينهما".

وفي عالم أطلقت فيه مؤخرًا وكالة الأمن الداخلي الإسرائيلية الشاباك برنامجًا خاصًا يسرّع بدء التشغيل فإن التعاون بين المجالَين العام والخاص سيزيد ففي الواقع عليها أن تتعاون لتواكب التطورات السريعة في مجالات مثل الذكاء الاصطناعي والتعلم الآلي وإنجازات أخرى في القدرات الحاسوبية

ولم تقم الحرب الالكترونية بتعتيم الخط الذي يفصل بين الهجوم والدفاع فحسب بل أيضًا مفهوم الملكية السيادية في ما يتعلق

بالتطور التكنولوجي - وبالتحديد ما يشكل بالضبط شركة إسرائيلية (او امريكية او صينية). لقد حجبت الإنترنت الحدود والحرب السيبرانية ليست مستثناة وكما قال شناير من جامعة هارفارد: "تُصنع الرقائق في (أ) وتُجمّع في (ب) وتكتب البرمجيات في جميع أنحاء العالم من قِبَل 125 فردًا من جنسيات مختلفة". وتبدو هذه الانسيابية شائعةً بشكل خاص في إسرائيل حيث أنشأت الشركات الأجنبية التي تملك أموالاً طائلة مراكز متقدمة لأنشطة الأبحاث والتطوير واشترت الشركات الناشئة المحلية

وفي حين أن الطبيعة الدولية لتكنولوجيا الحاسوب تعود بفوائد كثيرة تعقّد عملية التحقق من مصدر الهجوم السيبراني وبالتالي إنّ غياب تحديد المصدر يصعّب استجابة الحكومات وعدم وجود تهديد بالانتقام يجعل الردع عسيرًا إن لم يكن مستحيلاً وكتب ديفيد سانجر في مقال نُشر في صحيفة "نيويورك تايمز" مقتبسًا من كتابه "السلاح الأمثل: حرب وتخريب وخوف في عصر الإنترنت": "إنّ السبب في ظهور الأسلحة السيبرانية كأدوات فعالة لكافة الدول مهما كان حجمها يكمن في كونه طريقةً للعرقلة وممارسة السلطة أو النفوذ من دون إشعال حروب ومعارك قتالية".

وفي حين أن القطاع الخاص قد يكون قادرًا على دفع رواتب أعلى لشعبه ما يجعله يجتذب المواهب والبراعة التكنولوجية لا تزال الحكومة تحمل ورقةً رابحةً واحدة: القانون وهذا ما يعيدنا إلى مجموعة "إن أس أو" ومنصور المعارض الإماراتي فمن أجل أن تبيع مجموعة "إن أس أو" بشكل قانوني السلاح السيبراني الهجومي الذي استُخدم لاستهداف منصور كانت بحاجة إلى تصريح من ضابط منظم تصدير الأسلحة الإسرائيلي الموجود في وزارة الدفاع بهذه الطريقة على الأقل يتم تنظيم الأسلحة السيبرانية بشكل صارم مثل أنظمة الأسلحة الأخرى التي يبيعها الإسرائيليون لحكومات أجنبية وحيث لا يكون التعامل إلاّ مع الحكومات

وفي هذا الإطار قال يوفال ساسون وهو شريك متخصص في تصدير الدفاع في شركة المحاماة "ميتار" الرائدة في إسرائيل: "إن بيع أنظمة كهذه إلى مؤسسات غير حكومية مثل شركة أو أصحاب نفوذ سياسي غير قانوني إطلاقًا وتمامًا مثل بيع طائرة بدون طيار أو رشاش ينظر الضابط المنظم إلى المستخدم النهائي: أي هوية الحكومة وأعمالها فالأداء الوظيفي اختبار محوري". وفي حالة الإمارات العربية المتحدة ومنصور نصح **(https://www.yediot.co.il/articles/0,7340,L-4851376,00.html)** بعض المسؤولين في مكتب المنظّم بعدم بيع هذا النظام لدولة عربية وفقًا للصحيفة اليومية الإسرائيلية "يديعوت أحرونوت". وأفادت بأن الأسلحة الإلكترونية التي وافق عليها المنظمون أخيرًا كانت أضعف من تلك التي اقترحتها شركة "إن أس أو" وقالت إن بعض المسؤولين في وزارة الدفاع يعارضون الصفقة لأن التكنولوجيا كانت تُباع إلى بلد عربي ونقلت الصحيفة عن مسؤول رفيع المستوى في الوزارة قوله: "من العار أن يمنحوا تصريحًا كهذا".

وقالت **(https://www.timesofisrael.com/israeli-government-okayed-sale-of-spyware-that-exploits-iphones/)** شركة "إن أس أو" في بيان لها إنها تمتثل لجميع القوانين ذات الصلة وإنها "لا تشغّل البرنامج لعملائها وإنما تطوره فقط". قد يكون هذا الفارق مجرد خدعة ولكنه يقدم مثالاً آخر على الإشكالات المتعلقة بمسألة الدفاع والهجوم والخاصة والعامة: فيمكن استخدام الأدوات السيبرانية الخاصة نفسها التي تم توظيفها ضد أعداء الدولة مثل الصحفيين والمعارضين لاعتراض سبيل تجار المخدرات والإرهابيين أيضًا ففي الواقع في عام 2016 استعان مكتب التحقيقات الفيدرالي بشركة إسرائيلية منفصلة تُدعى "سيلبريت" لفتح جهاز آيفون الخاص بأحد الإرهابيين المتورطين بتنفيذ هجوم سان برناردينو في كاليفورنيا عام 2015 حيث استخدمت الشركة أداةً سيبرانيةً جديدةً لفتحه بعد أن رفضت شركة "آبل" أن تقوم بذلك ويقال **(https://www.haaretz.com/israel-news/business/.premium-inside-the-israeli-company-that-can-crack-the-iphone-1.5420595)** إن "سيلبريت" تبيع منتجاتها في أكثر من 100 بلد

وفي حين أن بعض المنتقدين يلومون إسرائيل على السلوك المارق فإن البلاد ليست بعيدة عن ذلك فلا يوجد في التجارة العالمية للأسلحة إلاّ قلة من الأولياء حتى بين الديمقراطيات الغربية ومن مصلحة الشركات الإسرائيلية الامتثال للقانون وتجنب التجاوزات ومنع وقوع التكنولوجيا في الأيدي الخاطئة وعلى حد تعبير أفنر "يمكن جني الكثير من الأموال وبشكل قانوني فلمَ العمل إذًا في الظلال "

وفي النتيجة لم تكن "إن أس أو" تعمل في الظلال فقد وافقت الحكومة الإسرائيلية على الصفقة التي أجرتها شركة خاصة في ما يتعلق ببيع أسلحة سيبرانية متطورة إلى حكومة عربية لديها مبادلات استخباراتية وأمنية وكان هذا القرار رمزيًا للطريقة التي تغيرت فيها التكنولوجيا والحرب والسياسة بشكل كبير خلال سنوات قليلة فقط ولطالما كان هناك عمليات تجسس وعمليات إعلامية وهجمات عسكرية وكذلك الجهات الخاصة التي تبيع الأسلحة في جميع أنحاء العالم (من بينها في العقود الأخيرة العديد من الأفراد العسكريين الإسرائيليين السابقين). أمّا الفرق الآن فهو مدى وصول الأدوات السيبرانية الجديدة وسرعتها وانتشارها السهل "لقد بدأ سباق التسلح السيبراني ذات الأبعاد التاريخية ولكن الخفية" بحسب سانجر - والسباق عالمي والجانب السلبي المحتمل واضح: سباق تسلح بدون قواعد أو معايير ومن دون خطوط أمامية واضحة لكن لا مجال للعودة

وقال بن أفرايم: "يجب أن نتواضع لقد بدأنا نفهمه للتو". وأضاف: "إنها ثورة حقيقية فقبل مئة عام لم يكن من عنصر جوي للحرب والآن بات عنصرًا حاسمًا لأي جيش". وقال: "الفضاء الالكتروني أكبر من ذلك حتى اليوم تفتح عينيك في الصباح – فتجد نفسك فيه".

نيري زيلبر زميل مساعد في معهد واشنطن ومؤلف مشارك (مع غيث العمري) للمقالة "دولة بلا جيش جيش بلا دولة: تطور قوات أمن السلطة الفلسطينية 1994-2018". ❖

"فورين بوليسي"

موصى به

BRIEF ANALYSIS

Iran Takes Next Steps on Rocket Technology

/ /

◆

Farzin Nadimi

(/policy-analysis/iran-takes-next-steps-rocket-technology)

تحليل موجز

السعودية تُعدّل تاريخها وتقلّص من دور الوهابية

فبراير

◆

سايمون هندرسون

(ar/policy-analysis/alswdyt-tudwl-tarykhha-wtqlws-mn-dwr-alwhabyt/)

BRIEF ANALYSIS

Targeting the Islamic State: Jihadist Military Threats and the U.S. Response

February 16, 2022, starting at 12:00 p.m. EST (1700 GMT)

◆

Ido Levy ,
Craig Whiteside

(/policy-analysis/targeting-islamic-state-jihadist-military-threats-and-us-response)

TOPICS

العلاقات العربية الإسرائيلية **(/ar/policy-analysis/allaqat-alrbyt-alasrayylyt)**

الطاقة والاقتصاد **(/ar/policy-analysis/altaqt-walaqtsad)**

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

انتشار الأسلحة **(/ar/policy-analysis/antshar-alaslht)**

الإرهاب **(/ar/policy-analysis/alarhab)**

المناطق والبلدان

إسرائيل **(/ar/policy-analysis/asrayyl)**

دول الخليج العربي **(/ar/policy-analysis/dwl-alkhlyj-alrby)**