التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

تقارير دولية

14

حرب الأفكار الجديدة
دروس في الأمن السيبراني

تقارير دولية

إصدار شهري يصدر عن الإدارة العامة للتخطيط والتنسيق

المشرف العام

اللواء الطيار الركن محمد بن سعيد المغيدي

الأمين العام للتحالف الإسلامي العسكري لمحاربة الإرهاب

رئيس التحرير

العقيد حسن بن سليمان العمري

مدير الإدارة العامة للتخطيط والتنسيق

التحرير والتصميم والإخراج

توق الإعلامية للأبحاث

TAOQ توق

البريد الإلكتروني: info@taoqresearch.org

هاتف: 114890124 966+

تقارير دولية

14

يونيو 2020

حرب الأفكار الجديدة

دروس في الأمن السيبراني

سعت الكاتبة كارا فريديريك إلى تفنيد كثيرٍ من الحمَلاتِ الرَّقْمية المغرضة والمضلِّلة، وحوادثِ القرصنة الإلكترونية، وتؤكِّدُ في مستهلِّ بحثها أن مستقبلَ النظام العالمي متعلِّقٌ بمقدار التأثير في الشعوب. ولطالما بقيَ المدنيُّون مادةَ الصراع المرير على مدًى طويل، بدءًا من التمرُّد، ومرورًا بالإرهاب، وانتهاءً إلى حرب المعلومات. إن التقنياتِ المستجدَّةَ تغيِّر قوانينَ اللعبة، وتحدِث ثورةً في عملية التأثير. وإن التقدُّمَ الذي أُحرِز على صعيد الذكاء الاصطناعي، ولا سيَّما في التعلُّم الآلي، يحوِّلُ المعلوماتِ إلى أسلحةٍ لممارسة الرقابة الاجتماعية على نطاق واسع. وقد استغلَّت بعض الأنظمة التقنياتِ الجديدةَ؛ لتُحكمَ قبضتها على شعوبها، باستخدام منصَّاتِ تواصل اجتماعي مراقَبة، وشبكاتٍ من الروبوتات، وتقنيةِ معرفة الوجه.

محاولات تقويض الثقة

تحاول جهاتٌ مُؤثِّرة خارجية تقويضَ ثقة الرأي العام بالنهج الديمقراطي، من طريق دعايةٍ محوسَبة، واستهدافٍ دقيق؛ بل إن جهات غيرَ حكومية تحاول تأجيجَ الاضطرابات السياسية بنشر معلومات مضلِّلة في مواقع الإنترنت. وهذه الأعمال تستهدف غالبًا النظام الليبرالي الحالي، ومؤسَّساته الداعمة، وتُنذر باضطرابات جيوسياسية محتمَلة. وهنا تشير الكاتبة إلى مخطَّطٍ لمقاومة هذا التهديد الخطِر، مستخلصًا من الدروس المستفادة من خوض حرب مختلفة؛ إذ إن الحرب على الإرهاب التي تلت الحادي عشر من سبتمبر قدَّمت خريطةَ طريق للمنظمات العامَّة والخاصَّة عن كيفية الاستجابة لمعركة من نوع آخر، هي معركة المعلومات.

وفي إطار الوعي التام بالتهديدات الإرهابية، تحركت كلٌّ من الحكومة الأمريكية وشركات القِطاع الخاصِّ في مواجهة الآخر في الفضاء الافتراضي والواقعي، وظهرت درجةُ الحدَّة والجدِّية لدى الحكومة الأمريكية فيما بين عامي 2002م و2017م، إذ كلَّفتها الحرب العالمية على الإرهاب 2.8 تريليون دولار تقريبًا من النفقات ذات الصلة، وما يقارب 16% من الإنفاق التقديري في المدة الزمنية نفسها. وهذا هو ثمنُ إستراتيجية نفي الخطر وتطويق الإرهاب قبل أن يصلَ إلى أرض الوطن، حيث يواجه الجيشُ الأمريكي الإرهابَ في ملاذاته الآمنة خارج الولايات المتحدة.

تأثر شركات التواصل الاجتماعي

كوَّنت شركاتُ الإعلام الجديد ومنصَّات التواصل الاجتماعي مجموعةً متضامنة لتنظيم محاربة الإرهاب، ولا سيَّما بعدما تبنَّى تنظيم داعش نشرَ مقطعٍ مصوَّر لقتل الصحفي الأمريكي جيمس فولي في يوتيوب وتويتر عام 2014م، ما فتح جبهةً جديدة أمام الشركات. وبحلول عام 2015م أجرت شركة فيسبوك التي كانت تعارض التشريعاتِ المتخاذلةَ في معالجة الإرهاب، عدَّة اجتماعات مع شركات تقنية أخرى لمناقشة فكرة منصَّةٍ لمكافحة الإرهاب. وفي مطلع 2016م مضى مسؤولون من البيت الأبيض ووكلاءُ رسميُّون إلى وادي السيليكون للقاء كبار قادة التقنية، وعلى رأسهم الرئيسُ التنفيذي لشركة آبل تيم كوك وممثلون لشركات: جوجل وفيسبوك وياهو وتويتر؛ لمناقشة وضع حلول للحدِّ من انتشار المحتوى الإرهابي في الإنترنت.

وفي العام نفسه أسهمت حاضنة «جيقسو» التابعة لشركة «ألفا بيت» في مواجهة تكتيكات المراسلات الداعشية عبر الإنترنت، وفي تنقية المحتوى على اليوتيوب، علمًا أن فكرة إنشاء الحاضنة تعود لشركة جوجل. وبحلول عام 2018م وظَّفت شركة فيسبوك 7500 موظفٍ بمناصب مديري محتوى، ومن أُولى مهامِّهم الوظيفية إبقاءُ المنصَّة الاجتماعية خاليةً من المحتوى الإرهابي. وفي السنوات الثلاث التي تلت تلك المناقشاتِ الأوليةَ عام 2015، أوقفت تويتر 1.2 مليون من حساباتٍ لمشتركين انتهكوا سياسات مكافحة الإرهاب.

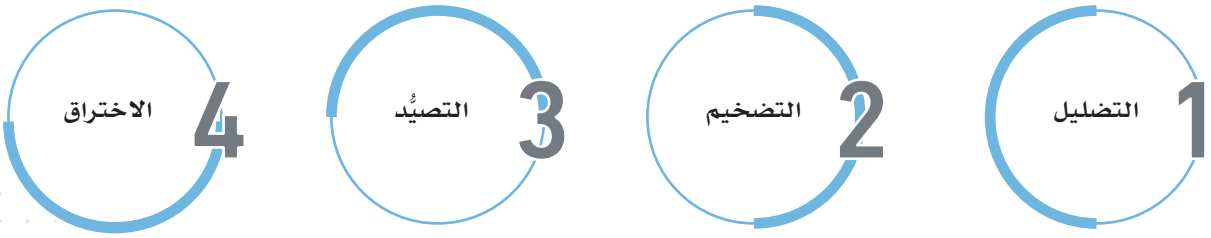
ومع بدء الحرب على الإرهاب بدأت شركات التقنية العملَ بنشاط على معاداة منصَّاتهم لمثلي الإرهاب، واستعانوا بالموهوبين والمميَّزين لسدِّ الثُّغرات ورفع الخبرات في مكافحة الإرهاب، مستحدثين مناصبَ جديدةً للتنسيق والإشراف على لوائح مكافحة الإرهاب العالمية. وتعاقدت مع أشخاص مؤثرين من ذوي الصلة في المنتديات الداخلية، وأسست لمجموعة من التدابير التقنية والتحليلات المهمَّة لاجتثاث المحتوى السيِّئ والمستخدِم المسيء. وتعاونت شركاتُ التقنية الكبيرة والصغيرة وبقوة القانون في تبادل أي معلومات متعلِّقة بتهديدات أمنية، وقامت بإعداد مُسَوَّدة للوائحَ لمنع إساءة الإرهاب لمنصَّاتهم الرَّقْمية على نحو خاص، وبتحديث التعليمات الداخلية لمجتمعاتهم، بالإضافة إلى دعمهم مبادراتٍ فكريةً لدحض الرسائل الدعائية الإرهابية.

وسائل حمَلات التأثير الخارجي

1) التضليل

يمكن تعريف حمَلات التأثير التي تعتمد على ترويج معلومات مغلوطة مضلِّلة: بأنها الاستخدام المنظَّم لمعلومات مكذوبة أو خاطئة، بهدف التشويش المتعمَّد والتضليل، أو تحويل الرأي العامِّ إلى أناسٍ مستهدَفين؛ لتحقيق أهداف إستراتيجية. وينبغي حتى نقاومَ أثر هذا النوع من المعلومات، أن نوليَ اهتمامًا خاصًّا للعملاء «الجهات المؤثِّرة»، ولعناصر التمكين «الأدوات والآليات» لحمَلات التضليل الرَّقْمي والتأثير الخارجي.

وسائل حمَلات التأثير الخارجي



أما ما يتعلَّق بالعملاء أو الجهات المؤثِّرة، فيواصل الباحثون ووسائل الإعلام والجمهور لفتَ الانتباه إلى حمَلات التأثير التي ترعاها بعض الدول بقيادة القوى الاستبدادية المعارضة فكريًّا لأنظمة الديمقراطية. وعلى سبيل المثال: إن الاستخدام الروسيَّ لعمليات التأثير بهدف تقويض التضامن عبر الأطلسي موثَّق جيدًا.

أما عناصرُ التمكين، فإن الجهاتِ المؤثِّرةَ تستطيع الجمعَ بين تكتيكات التضخيم، والاستهداف المصغَّر؛ لزيادة تأثيرها إلى أقصى حدٍّ ممكن. وفي تقييم نشاط الروبوت عبر الإنترنت أجراه عام 2016 الأمنُ السيبراني الأمريكي، وجد أن الروبوتات تبلغ أكثرَ من 50% من النشاط الحركيِّ على الإنترنت. وتستهدف الروبوتات السياسية الرأيَ العامَّ بتضخيم قصص مدمِّرة أو مشتِّتة للانتباه، عن طريق «حقول الأقزام، وهي مجموعاتٌ من مستخدمي الإنترنت ينسِّقون مشاركاتهم مع مستخدمين آخرين بقصد المضايقة والتضليل، وبثِّ معلومات غير صحيحة، وباستخدام روبوتات وسائل التواصل الاجتماعي، وهي شبكات مؤتمتة لحسابات مزيفة. وتقوم الجهاتُ المؤثِّرة بإخفاء آثارهم الرَّقْمية بانتحال (بروتوكول) شبكي. وكذلك يمكن استغلال البيانات الوصفية من قِبَل مستخدمي منصَّات الإنترنت، التي تستفيد منها الإعلاناتُ الدعائية لرسم صورة لسلوك المستهلك؛ لأغراض التضليل أيضًا.

2) التضخيم

من وسائل الحمَلات الخارجية المؤثِّرة تضخيمُ الاستقطاب السياسي؛ إذ يُتيح الاستقطاب السياسي مجالًا للكِيانات الأجنبية لتقسيم الجمهور الأمريكي، على سبيل المثال: في أعقاب حادثة إطلاق النار في مدرسة باركلاند الثانوية عام 2018م، سعت روسيا لتأجيج الجدل الدائر في الولايات المتحدة بشأن غياب قوانين السيطرة على الأسلحة، وذلك بإغراق تويتر بالتعليقات الجدَلية تحت وسم السيطرة على السلاح الآن guncontrolnow، وفتح المزيد من الوسوم لإثارة ردود فعل عاطفية.

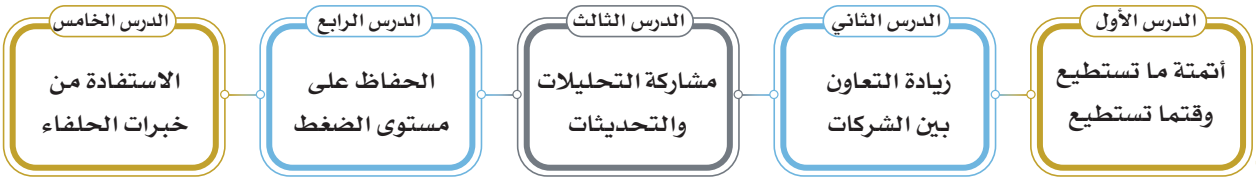
إن انخفاض حواجز الحماية في مواقع التواصل الاجتماعي والإعلام الجديد تجعل من الدخول إليها أمرًا سهلًا أمام الجهات الخبيثة لنشر محتوًى كاذب أو متحيِّز، ولبثِّ دعايات ممنهجة تعبث بالبيئة المعلوماتية. وكشفت دراسةٌ أجراها باحثون من معهد ماساتشوستس للتقنية عام 2018م أن انتشار الأخبار المغلوطة والباطلة على تويتر أسرعُ وأعمق أثرًا على نحو ملموس من انتشار الحقيقة، ولا سيَّما عندما يتعلَّق الأمر بالأخبار السياسية، وعزا الباحثون هذه النتيجةَ جزئيًّا إلى استثارة عواطف الناس.

3) التصيُّد

من سمات التصيُّد الإلكتروني الاحتيالي أنه يحاول خداعَ أشخاص محدَّدين، ويتقصَّد تثبيت البرامج الضارَّة بإرسال طلبات عبر البريد الإلكتروني تبدو ظاهريًّا أنها سليمة. ومن أمثلة التصيُّد الرَّقْمي: الهجوم عبر البريد الإلكتروني الذي أضرَّ بالمرشَّحة للرئاسة الأمريكية هيلاري كلينتون، عبر الإضرار برئيس حملتها الانتخابية جون بوديستا والمؤتمر الوطني الديمقراطي عام 2016م، بمساعدة نظام تمكين المعلومات الذي يتيحه الذكاء الصناعي. وتزداد صعوبة التفريق بين هذه الهجَمات الخادعة والرسائل الموثوقة، فضلًا عن أن القدرة على إجراء حمَلات تصيُّد إلكتروني بطريقة آلية واسعة النطاق ستزيد من احتمال نجاح المهاجمين.

وتستخدم حمَلات التأثير الخارجي «الأجنبي» نوعًا آخرَ من أنواع التضليل، وهو زرعُ معلومات خاطئة في حُزمة معلومات حقيقية صحيحة مقرصَنة، مما يُربك الثقةَ

دروسٌ من عضلة الذاكرة



في المرشَّحين الانتخابيين أنفسهم. من ذلك مثلًا: في إبَّان الحملة الانتخابية الفرنسية للرئيس إيمانويل ماكرون، في عام 2017م، وقعت حادثةٌ تعَدُّ اختبارًا ميدانيًّا واقعيًّا لهذه الآلية، فقد اخترق الروس شبكةَ الحملة، وسرَّبوا معلومات عن شراء أحد موظفي الحملة للمخدِّرات، وحاكوا نسيجًا متقنًا من المعلومات المغلوطة، مخلوطًا بالمعلومات الموثوقة، بهدف إرباك الجماهير الفرنسية، وقلب مواقفها من ماكرون.

4) الاختراق

تضرب حمَلات التأثير الخارجي في البُنى التحتية للعمليات الانتخابية التقليدية، وتحديدًا قبل عام 2016م، عندما أعلن مركز «برينان» التابع لجامعة نيويورك أن أكثر من ثلاث وأربعين ولاية تستخدم آلات تصويت قديمة، وأجهزة هواتف نقالة مرتبطة بشبكات إلكترونية سهلة الدخول وغير آمنة، ما قد يعرِّض عمليات الاقتراع وفرز أعداد المنتخبين لثُغرات قابلة للاختراق. وفي تقرير صدر عن المركز الأمريكي للتقدُّم عام 2018م، أُشيرَ إلى أن كلَّ ولاية تتخذ إجراءاتٍ أمنيةً سيبرانية جديدة منذ عام 2016م، وذلك من أجل تحسين إدارة الانتخابات النصف نهائية، ومع ذلك لا يزال هناك الكثيرُ من الفجَوات والتفاوت الواضح في مستويات التقدُّم.

دروسٌ من عضلة الذاكرة

التقنيات الرَّقْمية الحديثة محفوفة بنِقاط ضعف جديدة، ومصحوبة بسُبل حديثة للتخريب على الصَّعيدين المعرفي والرَّقْمي، إلا أن شركات التقنية والقِطاع العام تمتلك عضلةَ الذاكرة لمعرفةِ هُويَّة تلك المحاولات، ومحاصرةِ الفضاء الذي تنطلق منه الجهاتُ الخبيثة، ثم الردِّ بالقوة على مبادراتهم. وأوجدت تجربةُ مكافحة الإرهاب عضلةَ الذاكرة هذه، التي يمكن تلخيصُها في خمسة دروس هي:

الدرس الأول: أتمتة ما تستطيع وقتما تستطيع

في البدء، على شركات الإعلام الجديد والتواصل الاجتماعي حصارُ الفضاء الذي تمارسُ فيه الجهاتُ الأجنبية أعمالها الخبيثة، برفع جاهزية منصَّاتهم لتكونَ «معادية» تجاه المحتوى الإرهابي، ثم تطبيق الطرق الدفاعية على حمَلات مؤثِّرة برعاية الولاية. وللتضييق على التصرُّفات التي تتخذها حمَلاتُ التأثير الخارجي الأجنبي، كتلك الشروط التي تعمل بها شركة فيسبوك بوصفها «سلوكًا منسَّقًا»، بإمكان الشركات تبنِّي إجراءات محدَّدة في هذا السياق، منها تقليصُ استعمال الأسماء المستعارة، والاستناد إلى خطوات مشدَّدة للتحقُّق من الهُويَّة، مثل: فحص الحسابات التي تُظهر مؤشِّراتٍ آليةً أكثر من كونها بشرية، وتقييم نزاهة الحسابات. العمل بهذه السُّبل المختبرَة سابقًا في مكافحة الإرهاب للتقليل من قدرات الشبكات الخبيثة، يمكن تطبيقُها لخفض عدد الحسابات المزيفة التي تنشر معلوماتٍ مغلوطةً أو مكذوبة. وتنفِّذ شركتا جوجل وفيسبوك إجراءاتٍ مماثلةً في سبيل التصدِّي لوسائل نشر المعلومات المغلوطة.

أما تويتر فقد أوقف 70 مليون حساب نهائيًّا بين شهري مايو ويونيو 2018م. وكلما زادَ حجم البيانات وتنوُّعها في بيئة المعلومات، وتطبيق الأتمتة لتعديل المحتوى آليًّا، مع نَقْص التضخُّم، وتضييق الإسناد، قلَّت فرص المهاجمين في الوصول إلى فضاء الإنترنت.

الدرس الثاني: زيادة التعاون بين الشركات

التحدِّيات التي تواجهها الشركات ذاتُ العَلاقة هي في الغالب تحدِّياتٌ مشتركة في هذه المعركة العالمية الجديدة، ومن ثَم فإن الاتحاد في اتخاذ الإجراءات المناسبة أمر مهمٌّ جدًّا. فمثلًا فرضت شركة فيسبوك لوائحَ جديدةً وتقنياتٍ متطوِّرةً يتجاوز تطبيقُها الولايات المتحدة وكندا إلى ملايين المستخدمين في العالم.

وفي سبتمبر 2018م أخبرت رئيسةُ التشغيل في فيسبوك «شيريل ساندبرج» لجنةَ المخابرات في مجلس الشيوخ أن شركة فيسبوك تعمل عن كثَب مع أقرانها في الصناعة؛ لإحراز تقدُّم في معالجة مشكلة حمَلات التأثير الخارجية. وتعهَّدت كلٌّ من جوجل وفيسبوك وتويتر في الشهر نفسه بالعمل معًا لمحاربة الأخبار المزيفة في أوروبا، ما يُعَدُّ اختبارًا لتعميم التجربة، وتوسيع نطاق هذا التعاون عالميًا. ومن الضروريِّ إدراكُ أن تعاون الشركات فيما بينها أمرٌ حاسم لا مفرَّ منه، وأن بعضهم أطلق نماذجَ معتمدة وجاهزة للاستعمال بين منسوبي الصناعة أنفسهم. ويجيء ذلك نتيجةً للجهود المبذولة في مكافحة الإرهاب، وينبغي عليهم الاستفادةُ منها، وتطويرها إن لزم الأمر.

الدرس الثالث: مشاركة التحليلات والتحديثات

ثَمَّ مكوِّن جوهريٌّ في مكافحة الشبكات الخبيثة وممثليها، ينبغي التنبُّه له، هو كيفية تنظيم صفوف المعركة وأدواتها. ولمَّا كان قِطاع التِّقانة عاملًا رئيسًا في حروب المستقبل، فإن الاعتماد على الإنجازات الماضية يمكن أن يسدَّ الفجوة بين القِطاعين العام والخاص، عبر الخبراء الذين تجمعهم أهدافٌ مشتركة. وهذه الأطُر وأنظمة التكامل موجودةٌ حقًّا، ويمكن القياسُ عليها. على سبيل المثال: أُنشئَ المركز الوطني لمكافحة الإرهاب في شمال فيرجينا عام 2004م؛ لتحسين نظام مشاركة المعلومات، وتحسين القدرات التنبُّئية بالتهديدات الإرهابية وسرعة الاستجابة لها. لذا يقترح الخبراءُ محاكاةَ الفكرة، وإنشاء مؤسسة مشابهة، تقوم بالوظيفة نفسها؛ لمواجهة عمليات التأثير الخارجية الأجنبية.

وتنصُّ التوصيات على ضرورة تعيين هيئة تضمُّ أعضاءً من وكالة المخابرات؛ لمقاومة الإرهاب، بالتنسيق مع القِطاع الخاص، تُعنى بإنشاء خلايا أصغر حجمًا، وأكثر ميلًا إلى التحرُّك والاندماج بسهولة، تحت إشرافها وتمويلها، وتُعنى بالتعامل رَقْميًا مع حمَلات التأثير الأجنبي الخبيث. وهنا ينبغي على شركات التواصل الاجتماعي أن تولِيَ هذه الجهودَ عنايةً خاصَّة، وأن تزوِّدَ هذه الخلايا الصغيرةَ بخبرات محلِّليها المتخصِّصين في مقاومة الإرهاب.

الدرس الرابع: الحفاظ على مستوى الضغط

لا تزال الحاجةُ ماسَّةً إلى مزيدٍ من الضغط، على الرغم من الأداء الجيد للحكومة وشركات التِّقانة، ولكن سيواصل الإرهابيون إيجادَ طرق مبتكرة للإساءة المجتمعية، عبر منصَّات التواصل الاجتماعي ووسائل الإعلام الجديد، وستواصل شركات التواصل الاجتماعي توظيفَ محلِّلين ومراجعين متخصِّصين في الإرهاب لمواكبتهم. وفي حين توفِّر إمكانيةُ نقل هذه الأدوات لمكافحة الإرهاب والتِّقنيات بدايةً مفيدة، تبقى مشكلة المعلومات المغلوطة المضلِّلة وآثارها الواسعة في المؤسسات الديمقراطية تفرض حاجةً ملحَّة لاتخاذ موقف استباقي باستمرار.

تغذِّي الأكاذيب والأخبار المضلِّلة الأنظمةَ الديكتاتورية، التي تحكم بالقوة والخوف، في حين تعَدُّ الحقيقة نقطةَ اتصال، ومطهِّرًا من الفساد والاستبداد في المجتمعات الحرَّة. تجد بعضُ الأنظمة نفسها مجبرةً على تغليف الواقع بالزيف، كي تحافظَ على السلطة، مثلما يحدث في المجتمع المتناغم بالنظام الصارم. ونجد على الجانب الآخر الأنظمةَ الديمقراطية تتيحُ للناس سبلَ الوصول إلى الحقيقة. وإذا كانت الأنظمة الاستبدادية تقوم على الأكاذيب لتُحكِم قبضتَها بقوة، فإن هذا يجعل من الحقيقة سلاحًا في وجه القمع. فعندما تسود الحقيقة تنتصر الديمقراطية.

الدرس الخامس: الاستفادة من خبرات الحلفاء

إن جميع الجهود والخُطط تستند إلى ميزة مهمَّة غير مستثمرة على النحو المطلوب، ألا وهي الحلفاء. وقد حقَّق إسهامُ حلف الناتو في الحرب على الإرهاب تعزيزَ جمع الاستخبارات، وقيادة عمليات في «عملية الحرية الدائمة» بأفغانستان. وأصبح حلف الناتو عضوًا رسميًا في التحالف العالمي لهزيمة داعش في مايو 2017م، وعضوًا في خلية الاستخبارات الإرهابية للمعلومات، التي تتخذ من بروكسل مقرًا لمكتبها الرئيس. وفي مواجهة التهديدات الأمنية في أفغانستان تتَّحدُ 38 دولة فضلًا عن الولايات المتحدة في تمويل قوات مساندة لعمليات مكافحة الإرهاب.

وينبغي على الولايات المتحدة دعوة حلفاءَ ديمقراطيين إلى تبادل أفضل الممارسات، من وحي تجربتهم الخاصَّة

في مواجهة حمَلات التأثير الأجنبي؛ لتخفيف القيود على التدابير السيبرانية الهجومية. ويجب على الولايات المتحدة أيضًا استخدامُ طريقة مجدية لتزويد القيادة السيبرانية بنتائج تبادل المعلومات، وتقديم توصيات عملية قابلة للتنفيذ.

ملخَّص

بعد الحادي عشر من سبتمبر تغيَّرت ساحة الحرب على الإرهاب؛ إذ بتنا في مرحلة جديدة سمِّيت عصرَ مكافحة الإرهاب، وهذا التغيير قد طالَ قاعات شركات التِّقنية الأمريكية، تقول الكاتبة: «اليوم، تشارك الولايات المتحدة في صراع توسعي، يتطلَّب تدخلًا من المؤثرين الرئيسين أنفسهم، شركات التقنية في القِطاع الخاصِّ والحكومة الأمريكية. ولم يعُد بمقدورهم تحمُّل تكرار الخطأ، وتفويت الكثير من الدروس المكتسَبة على مدار عِقدين من الزمن في مكافحة الإرهاب، من النواحي الإستراتيجية والتِّقنية والتنظيمية». وإن الاستفادة من تجارِبَ ناجحةٍ في قِطاع التِّقنية وجهود الحكومة الأمريكية لمكافحة الإرهاب تعزِّز من قدرة الولايات المتحدة على تحدِّيات التضليل الرَّقْمي في المستقبل.

وهناك خمسة دروس ينبغي على القِطاعين الخاصِّ والعامِّ الاستفادة منها باهتمام وعناية في سبيل مكافحة الإرهاب، وهي:

1- تطوير طرق تقنية لمعرفة المحتوى المؤثر للحمَلات الخارجية.

2- زيادة التعاون بين الشركات.

3- التمازج بين قِطاعَي التقنية والحكومة؛ بمشاركة التحليلات والتحديثات.

4- الحفاظ على اليقظة ووضع الهجوم، وتوظيف الموارد الضرورية لإلحاق الأذى بالخصوم أو إبقائهم في موقف دفاعي.

5- الاستفادة من خبرات الحلفاء.

في المجمل تُسهم المجموعة الآتية من الوصايا في مكافحة الحمَلات الخارجية المؤثرة في ضوء هذه الدروس الخمسة المستفادة، الوصيَّتان الأُولَيان تستهدفان القِطاعَ الخاص لصناعة التِّقنية، في حين تُعنى الوصية الثالثة بقِطاع الصناعة والحكومة الأمريكية، والوصيَّتان الأخيرتان موجَّهتان للوكالات الحكومية الأمريكية.

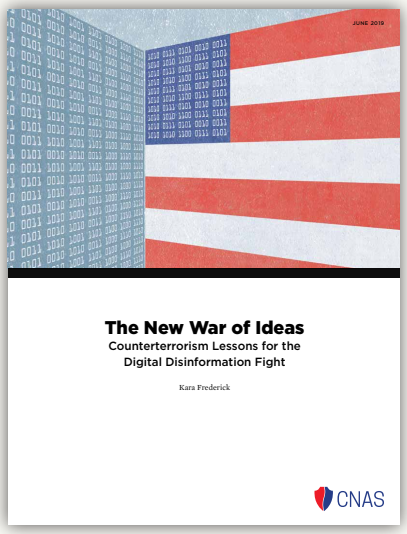
التوصيات

- على شركات التقنية، على المدى البعيد، توجيهُ نسبة دائمة من طاقتها الهندسية إلى أتمتة البحث عن هُويَّة الحمَلات الخبيثة المؤثِّرة. على سبيل المثال: تستطيع الشركات الحصولَ على قوة تأثير كبيرة بتوظيف الممارسات والتقاليد في التطبيقات، مثل: حدث (الهاكاثون) في الفيسبوك، عبر اجتماع مبرمجي الكمبيوتر لتبادل خبرات ومهمَّات هندسية وبناء نماذج أولية، والسعي للتوصُّل إلى إصلاحات تقنية لمشكلة التضليل المعلوماتي.
- على شركات التقنية إنشاء جمعية مختصَّة بالتضليل المعلوماتي، وتمويلها، لتنضمَّ إليها الشركاتُ الراغبة التي أُنشِئت بعد منتدى الإنترنت العالمي لمكافحة الإرهاب (GIFCT)، تتولَّى الجمعية وضعَ معاييرَ خاصَّةٍ بالصناعة، وتتبُّع حمَلات الشركات ذات التأثير الخبيث والمضلِّل.
- على مكتب مدير المخابرات الوطنية (ODNI)، بالتنسيق مع القِطاع الخاص، تعيينُ هيئة من ممثِّلي الوكالات لإنشاء خلايا دمج أصغر حجمًا، وأكثر ميلًا إلى التقدُّم، وتمويلها، تجمع هذه الخلايا بين محلِّلي القِطاعين العام والخاص. وإن شركات الإعلام الجديد أو التواصل الاجتماعي مطالبة بالإفادة من موظفيها، الذين يشتغلون على تحليل التهديدات المخابراتية، مع وكالات الاستخبارات؛ لتقديم تحاليل إلى هذه الهيئة، وفتح حوار متواصل، مع الالتزام بما يناسب كلَّ حوار من مستويات التصنيف السرِّي وغير السرِّي. وفي حال أظهرت الهيئة مؤشِّراتٍ محدَّدةً للنجاح، فعلى الحكومة الأمريكية النظر في تخصيص قوة مستقلَّة، وبأعلى مستوى مشترك، بهدف إيجاد الانسجام بين هذه الخلايا، وتولِّي جميع المسؤوليات لمواجهة أيِّ عمليات رَقْمية خارجية مؤثرة.

- على السلطة التنفيذية توسيعُ إستراتيجية الأمن السيبراني، وصلاحيات القيادة السيبرانية الأمريكية، بالقيام بعمليات هجومية تتسبَّب في خسائرَ للخصوم.
- على الحكومة الأمريكية العملُ مع حلفائها الديمقراطيين على تبادل الممارسات والخبرات في تطويق التأثير الخارجي للحمَلات الهجومية، مع الاستفادة من خبراتهم في اتخاذ إجراءات سيبرانية هجومية. ويجب استخدام وسيلة التأسيس ذاتها، لتكونَ طريقةً رسمية لتقديم نتائج مشاركة هذه المعلومات، مع وصايا للعمل.

الكاتبة

كارا فريديريك Kara Frederick، قضت ستَّ سنوات محلِّلةً في مكافحة الإرهاب بوزارة الدفاع الأمريكية، وعملت كبيرة محللي الاستخبارات الحربية الخاصة التابعة للبحرية الأمريكية، وأسهمت في تكوين أول فريق أمن سيبراني عالمي في شركة فيسبوك، وعملت قائدة لفريق الاستختبارات الإقليمي بمقر فيسبوك في كاليفورنيا. وتشغل حاليًا منصبَ زميل مساعد في برنامج الأمن الوطني والتقني بمركز الأمن الأمريكي الجديد (CNAS). وهي حاصلةٌ على «بكالوريوس» في التاريخ والشؤون الخارجية من جامعة «فيرجينيا University of Virginia»، وعلى «الماجستير» من جامعة «كينغز كوليج King's College» في لندن في الدراسات الحربية.



حرب الأفكار الجديدة
دروس في الأمن السيبراني


التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION


التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION