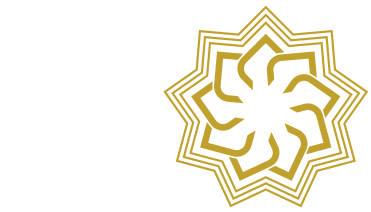
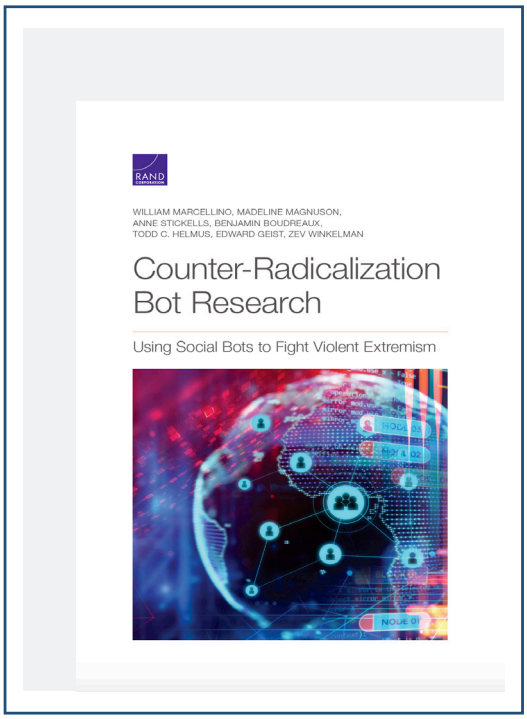
مرادات



تقارير دولية

أبحاث بوتات مكافحة التطرف

توظيف البوتات في محاربة التطرف العنيف



العـــدد
27

2021

يوليو

www.imctc.org

تقارير دولية

إصدار شهري يصدر عن التحالف الإسلامي العسكري لمحاربة الإرهاب

المشرف العام

اللواء الطيار الركن محمد بن سعيد المغيدي

الأمين العام للتحالف الإسلامي العسكري لمحاربة الإرهاب / المكلّف

رئيس التحرير

عاشور بن إبراهيم الجهني

مدير إدارة الدراسات والبحوث

ملاحظة: الأفكار الواردة في هذا التقرير تُمثّل رأي الجهة المصدرة له ولا تُمثّل رأي التحالف بالضرورة

التحرير والتصميم والإخراج

توق الإعلامية للأبحاث

البريد الإلكتروني: info@taoqresearch.org

هاتف: 966 114890124+

أبحاث بوتات مكافحة التطرف

توظيف البوتات في محاربة التطرف العنيف

صدرَ هذا التقرير: «**أبحاث بوتات مكافحة التطرف**: توظيف البوتات في محاربة التطرف العنيف Counter-**Radicalization Bot:** Using Social Bots to Fight Violent Extremism»، عن **مؤسسة راند RAND**، وهو من إعداد: ويليام مارسيلنيو، ومادلين ماغنُسون، وآن ستيكلز، وبنيامين بوردوكس، وتود سي هليموس، وإدوارد غايست، وزيف وينكلمان. ويتناول برامجَ روبوتات الإنترنت المعروفة بالبوتات، ويقوِّم إمكانية توظيف الحكومة الأمريكية لها في مكافحة التطرف والإرهاب.

يتألف التقريرُ من **خمسة أقسام**: التعريف بتقنية البوتات، والوضع الحالي لاستخدامها في مجالات شتَّى، والقضايا الأخلاقية والقانونية المتعلِّقة بتوظيفها، وتطوير مفاهيم توظيف البوتات، وأخيرًا توصيات مقدَّمة للحكومة الأمريكية. وقد اعتمد التقريرُ على عدَّة لقاءات مع الخبراء المختصِّين في الموضوع، إضافة إلى مراجعة الأدبيات القانونية والأخلاقية المتوافرة، وحالات الاستخدام السابقة لهذه التقنية وأثرها في الأفراد، وجمع البيانات، وحمَلات الرسائل. ومع عنايته واهتمامه بالجماعات الإرهابية، مثل: تنظيمَي القاعدة وداعش الإرهابيين، فهو أيضًا قابل للتطبيق على ما يماثلهما أو يشابههما من جماعات.

البوتات وأنواعها

البوتات أو روبوتات الإنترنت، هي برامجُ إلكترونية تحمَّل على مِنصَّات التواصل الاجتماعي، وتعمل منفردة آليًا، أو تعزِّز من عمل الإنسان (المرسِل)، وتضمُّ في عملها تقنيَّات الذكاء الاصطناعي، والإدراك الاجتماعي، والقدُرات اللغوية. وتُستخدَم لأغراض متنوعة بطرائقَ مختلفة؛ كالتأثير في المستخدمين، وإمدادهم بمعلومات عن الموضوع الذي يدعمه البوت، أو إيهام المستخدمين بأن موضوعًا ما يَلقى دعمًا كبيرًا وواسعًا، أو إحداث ضجيج إلكتروني للتشغيب على قضية ما، أو تشتيت المستخدمين وتوجيههم في الاتجاه الخاطئ؛ بإعطاء معلومات أو بيانات بديلة.

وقد تعمِدُ البوتات إلى التضليل المباشر، وبناء خطابات و«سرديات» زائفة، أو الربط بين المستخدمين من ذوي الاتجاهات والآراء والاهتمامات المتماثلة والمتشابهة، أو التحرش بالمستخدمين لدفعهم بعيدًا عن ساحة التواصل الاجتماعي، أو إنشاء صداقة مع مستخدمين للولوج إلى بيانات مستهدَفة، أو إقناع المستخدمين بأن البرنامج هو عبارة عن مستخدمٌ بشري؛ ليمنعَ تواصلهم مع مستخدم حقيقي.

وقد تمكَّنت الجماعاتُ المتطرفة مثل تنظيم داعش الإرهابي والتنظيمات اليمينية في الغرب، من استخدام هذه التقنية لنشر أفكارها في الفضاء السيبراني، وتجنيد أعضاءٍ جدُد، وتوسيع نطاق التأييد لها. من هنا كان توظيف هذه التقنية للحدِّ من تأثير هذه الجماعات ضرورة، وهي أداةٌ مؤثرة تستطيع الجهاتُ المختصَّة بمكافحة التحوُّل إلى الأصولية والتطرف العنيف استثمارها. إلا أن هذا التوظيفَ تتوقف نتائجه على عواملَ عدَّة؛ كمراعاة القيود التقنية، والشؤون القانونية والأخلاقية.

بدأ استخدامُ روبوتات الإنترنت أو البوتات الاجتماعية في مرحلة مبكِّرة من تطوُّر الإنترنت، في عِقدَي الثمانينيات والتسعينيات؛ لأغراض محدودة، كالألعاب وإدارة غرف المحادثات. وأصبحت بعض الحكومات والجيوش والسياسيين يستخدمون البوتات للعبث في الرأي العام، وتوجيه النقاشات عن مسارها الطبيعي على مختلِف منصَّات التواصل الاجتماعي. وقد أقرَّ موقع (تويتر) بأن نحو 23 مليون حساب من حساباته هي مجرَّد «بوتات»، وبيَّن موقع (فيسبوك) أن الحسابات المزيفةَ لديه في إحدى السنوات بلغت من 5% إلى 6% من إجمالي الحسابات فيه.

إن ظهور منصَّات التواصل الاجتماعي مثل فيسبوك وتويتر، واندماجها بتقنيات الذكاء الاصطناعي والتعلُّم الآلي، أدَّى إلى الثورة الحالية في عالم الاتصال. وزاد تأثيرُ هذا التواصل في مجالات شتَّى كالسياسة والاقتصاد، إضافة إلى تحقيق هدفها الرئيس. وأخطر الآثار يتجلَّى في نجاح الجماعات المتطرفة العنيفة في تسخيرها لتحقيق أهداف الدعاية، والتجنيد، والتأثير، على نحو يفوق الوسائلَ المستخدمة في محاربة هذه الجماعات. وتعمِدُ جماعات مثل داعش إلى الوصول إلى الأشخاص الأكثر تأثرًا بفكرها وميلًا إلى منهجها، عبر المحادثات والرسائل المفتوحة، ثم تسعى إلى إدخالهم في مجموعات خاصَّة سرِّية من أجل تجنيدهم. وهذا يجعل اكتشاف المجنَّدين قبل تحوُّلهم إلى الأصولية أمرًا شديدَ الصعوبة.

البوتات الأمينة

تتيح منصَّات التواصل الاجتماعي عبر «واجهات البرمجة على التطبيق» فرصًا لمطوِّري البوتات لاستغلال إمكانات هذه المنصَّات. مما دفع الكثيرَ من المعلنين التجاريين إلى استخدام البوتات تجاريًا، بطريقة لا تعارض شروطَ استخدام هذه المنصَّات. وتُعرَف هذه البوتات بـ **البوتات الأمينة**؛ لأنها لا تدَّعي أنها مستخدم حقيقي.

وفي بداية عام 2018م بدأت هذه المنصَّات عملية تطهير؛ لطرد «البوتات» التي تدَّعي أنها مستخدم حقيقي، أو حسابات مزيفة، مما أدَّى إلى ما يشبه سباق تسلُّح بين المنصَّات ومطوِّري البوتات. ومثال ذلك: تفعيلُ موقع فيسبوك نظام الحماية الخاصَّ به، القائم على تقنيات التعلُّم الآلي، التي تراجع أكبرَ قدر من الحسابات، وما يُشَر فيها، وإيقاف البوتات.

وأوضحت دراسةٌ صادرة عن جامعة كولومبيا البريطانية أن «الفيسبوك» لم يُوقف إلا 20% من البوتات، حتى بعد أن أَبلغ عنها عددٌ كبير من المستخدمين. في حين نجح موقع «تويتر» في تقليل تأثير البوتات التي استخدمتها بعضُ الأطراف في روسيا لإحداث ضجيج إلكتروني في أثناء انتخابات 2011م. وتمكَّن مطوِّرو البوتات من التغلُّب على تقنية ربط الحسابات بعُمر المستخدم؛ لاكتشاف المستخدم، وذلك عبر شراء بعض الحسابات الحقيقية، مما أدَّى إلى تطوير تقنية لاكتشاف السلوك الاجتماعي للحسابات.

ويستنتج الباحثون أن معظم البوتات المستخدمة حاليًا بوظائفها ووسائلها المختلفة لها تأثيرٌ سلبي في الفضاء السيبراني، وقليل منها يُستخدَم لإحداث أثر إيجابي، وربما يكون هذا استثناءً قياسًا إلى البوتات التي تستهدف بيعَ السلع، أو سرقة المعلومات الشخصية، أو نشر الأفكار الدعائية. ويعزو الباحثون هذا

الأمر إلى صعوبة المشاركة الإيجابية مع المستخدمين البشر، وما تسبِّبه من سوء في التفاعل. وقد يؤدِّي التطوُّر في مجال الذكاء الاصطناعي إلى بناء بوتات أكثر تطورًا تُسهم في الخير العام للمجتمعات، وقد يحدث هذا التقدُّم بتطوير تقنيات مختلفة، مثل تعرُّف الخطاب بدرجة عالية الدقة، وتوليد اللغة الطبيعية وفهمها، بما يجعل البوتات قادرةً على إجراء محادثة مع مستخدم بشري، وفهم جميع كلماته ودلالاتها.

إلا أن التحدِّيَ في هذا الصدد هو في عجز تقنيات التعلُّم الآلي المتوافرة حاليًا عن المشاركة في مثل هذه المحادثات في العالم الحقيقي، دون أن تستغنيَ عن المُدخَلات من البيانات، وهذا يجعل لغتَها أقرب إلى تمثيل المعرفة لا إيجادها. ولتعويض هذا العجز يقترح الباحثون اعتمادَ التخطيط الآلي لتحديث الخطاب الذي تستخدمه البوتات في التصدِّي لبرامج المراسلة التي يستخدمها الخصوم. وقد تصبح هذه العمليةُ مخططًا سيبرانيًا يضع إستراتيجية لتوظيف الخطاب بمراجعة الخطابات المنتشرة في الإنترنت. ويرى بعضُ الباحثين أن إمكانات الذكاء الاصطناعي الحالية قد تتطوَّر إلى التعلُّم العميق بما يجعل العامل البشري غيرَ مهم. لكنَّ الفجوة الكبيرة في «أدبيات» قضايا الذكاء الاصطناعي وتطبيقاته، تُظهر الحاجة الملحَّة إلى مزيدٍ من الجهد البحثي القادر على تحقيق نُقلة في إنتاج اللغة الطبيعية وفهمها.

خريطة التوظيف

تناول التقرير الوضعَ الحالي لاستخدام البوتات بوظائفها المختلفة، في مجالات شتَّى تتنوَّع بين مجالات الصحة والاستخدام السياسي. وهناك حالاتٌ ناجحة لاستخدام البوتات في المجال الصحي للقيام بالوظائف العاطفية الضرورية لمتابعة حالات المرضى، وبعضُها يكون ثلاثي الأطراف، يشترك فيه البوت والمريض والمعالجون المختصُّون، مثل: «بوت ميلودي» و«بوت بابليون»، اللذَين يجمعان المعلومات من المرضى، ويوصيان المعالجين باتخاذ إجراءات معينة. وقد يُعزى الأداء الإيجابي لهذه البوتات إلى العامل البشري، وضيق مجال الخبرة المطلوبة لتفعيل هذه البوتات، والبيئة المنضبطة والمحكمة التي تُطلَق فيها.

أما «**بوتات المقابلة**» فتعمل على الربط بين مستخدمين لا يمكنهم أن يتعارفوا فيما بينهم مباشرة. على سبيل المثال: يقوم «بوت سينساي» بالربط بين المستخدمين الذين يحتاجون إلى سلعة أو خدمة ما. كذلك طوَّر معمل الإعلام بمعهد ماساتشوستس للتقنية ما يُعرف بـ «بوت بكوكو» للربط مباشرة بين الأشخاص الذين يعانون أعراضًا متشابهة من القلق والاكتئاب، ويستهدف البوت الشبابَ النشيطين على منصَّات التواصل، والتطبيقات المفردة المخصَّصة للتعامل مع هذه الأمراض.

ومن الطرائق التي تربط بها البوتات المستخدمين بعضَهم ببعض؛ البحثُ في سجلِّ المحادثات عن كلمات محدَّدة، أو الاستجابة إلى رسائلَ معينة. وقد أوضحت إحدى التجارِب أن المستخدمين لبرامج الرسائل أكثر ميلًا إلى الحسابات التي يبدو أنها أكثر تأثيرًا، أو تلك التي تنتمي إلى المجموعة العِرقية أو الاجتماعية التي ينتمون إليها. وأوضحت تجارِبُ أخرى أن النوع الاجتماعي الذي يبني عليه البوت شخصيَّته يؤثر في

مقدار جاذبيته للمستخدمين. كذلك تُؤثر عواملُ متعلِّقة بحجم التغريدات ومعدَّلها، وطرق توليد التغريدات، واستهداف مجموعة معينة من المستخدمين في نجاح البوتات.

وتحاول بعض البوتات الأخرى التي يُطلَق عليها «**بوتات الحصاد**» أن تجمعَ أكبر قدر من المعلومات الخاصَّة بالمستخدمين. وتعمل هذه البوتاتُ بطريقة سهلة؛ ففي الفيسبوك مثلًا تُرسِل طلبات صداقة إلى المستخدمين، وعند قَبول طلباتها تقوم البوتات بجمع كلِّ ما هو مُتاح في الملفَّات الشخصية للمستخدمين من أخبار ومنشورات وتنويهات وتنبيهات. ويبدو أن الهدف من هذه البوتات جذبُ المتابعين والمستخدمين. وغالبًا ما تستخدم هذه البوتات صورًا شخصية لنساء جميلات، وكثيرًا ما تَلقى طلباتُ الصداقة المرسلة من تلك الحسابات الوهمية قَبولًا وجاذبية. وقد أطلق حِلفُ الناتو على هذه البوتات اسم «ترول البيكيي» أو «**بوتات المتعة**».

ويجري التحكُّم في سلوك البوتات كليًا بواسطة العامل البشري، ويمكن أن يتجاوزَ البوت جمعَ البيانات إلى إجراء محادثات خاصَّة مع المستخدم، ثم دفعه إلى المشاركة في عدد من الأنشطة؛ كأنواع من التجارة غير المشروعة، أو تدمير نظام التشغيل الخاصِّ به، أو إصابته ببرامج ضارَّة. وقد تمكن فريقٌ بحثي بجامعة كولومبيا البريطانية في عام 2011م في شهرين فقط من استخدام 102 من الحسابات الذاتية (ترول) على موقع الفيسبوك، واستخلصوا في مدَّة يسيرة 250 جيجا من البيانات، من أكثرَ من 3000 مستخدم.

وأثبتت بعضُ التجارِب إخفاقًا في التعامل مع المستخدمين، ومن ذلك «**بوت المحادثة**» الخاصَّة بشركة مايكروسوفت، والمعروف بـ (بوت «تاي») الذي تجاوز العجزَ عن تحقيق الأهداف المرجوَّة منه إلى إحداث آثار عكسية غير مرغوبة. وقد أُطلق البرنامج في عام 2016م ووصفته الشركةُ بأنه برنامج تعلُّم آلي بتحليل أنماط التفاعل في الرسائل بين المستخدمين، إلا أنه سَرعانَ ما طوَّر البرنامج لغةَ محادثة عنصرية، مما أدَّى إلى إيقاف البرنامج بعد يوم واحد من إطلاقه على موقع تويتر. في المقابل نجح برنامج الذكاء الاصطناعي المعروف بـ (شياويس Xiaoice) عندما أطلقته شركة مايكروسوفت نفسُها على منصَّة (وي تشات) الصينية، واكتسب شعبيةً واسعة، وجرت إضافته إلى مليون ونصف من مجموعات المحادثة، ودخل في محادثات مع عشرة ملايين مستخدم دون إحداث أيِّ ردود فعل غاضبة.

والفرق بين أداء البرنامجين يظهر بوضوح في إطلاق (تاي) على منصَّة عامة وهي تويتر، وإطلاق (شياويس) على منصَّة محادثات خاصة، إلا أن الفرق الأهمَّ هو السياق الاجتماعي والسياسي لإطلاق البرنامجين. فالمستخدمون على تويتر (الشائع استعماله في الولايات المتحدة والغرب) يميلون إلى استخدام لغة حادَّة وربما هجومية، أما في الصين فقد أدَّت الرقابة الحكومية الصارمة على المحتوى إلى رقابة ذاتية لدى المستخدمين على كلِّ ما يتحدَّثون به، وعلى اللغة المستخدمة.

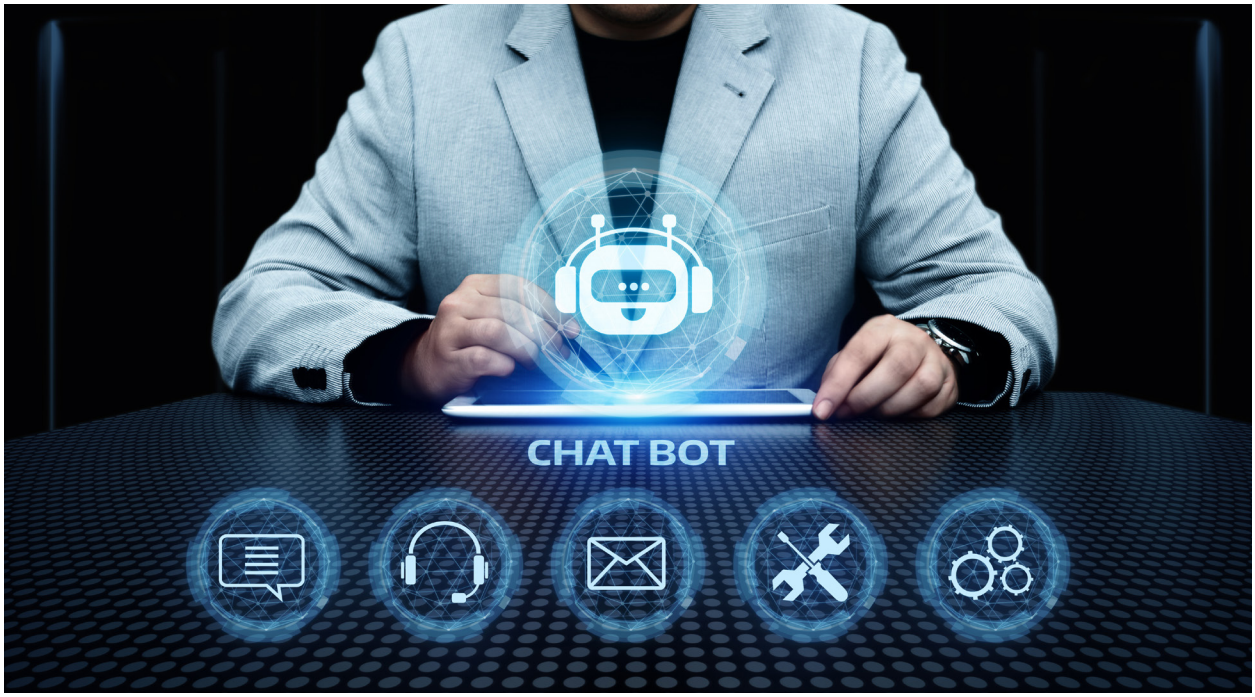
ومن البوتات ما يُستخدَم لنشر الأخبار، أو للتضليل، أو لتثبيت رؤية محدَّدة، وتعمل هذه البوتات عبر وَحدة شبكية، مما يجعل لها قوةً وتأثيرًا كبيرين. وهذا النمطُ من البوت الذي يختلط بالترول استخدمته روسيا على نطاق واسع؛ للتأثير في خيارات الناخبين الأمريكيين في انتخابات عام 2016م.

أما (بوتات الأستروترف) فتُستخدَم عندما يدفع لها الأفرادُ للحصول على شعبية أو تأثير أبعد مدًى وأوسع انتشارًا. وقد اتُّهمت حملةُ السياسي «ميت رومني» في الانتخابات الأمريكية عام 2012م بشراء المتابعين بواسطة هذا البوت، وأسهم ذلك في إثارة الشكوك بحملته الانتخابية. إلا أن الأحزاب السياسية في المكسيك نجحت في توظيف البوتات في انتخابات 2012م نجاحًا كبيرًا، بسبب القيود على الإعلام الرسمي والمؤسسي، ولا سيَّما القضايا المتعلِّقة باتفاقيات تجارة المخدِّرات. وأدَّى هذا الاستخدامُ من قِبَل الحزب الثوري الحاكم في البلاد منذ مدَّة بعيدة إلى حرب ضَروس قادتها حملةُ بينيا مرشَّح الحزب الرئاسي للتشنيع على المنافسين، وتمكَّن البوت المعروف بـ (بوت بينيا Peñabot) من التأثير في الوسوم المعادية أو المعارضة لسياسات بينيا، وأوجد مساراتٍ أو وسومًا «هاشتاقات» حقَّقت انتشارًا واسعًا «ترينداتٍ»؛ لتوجيه النقاش في اتجاهات معينة.

قياس النُّضج

كشف التقريرُ أن تقنية البوتات قد تطوَّرت في الآونة الأخيرة تطورًا كبيرًا ملحوظًا، ويتضح من النماذج المعروضة أن وظائف البوتات وأنواعها وكفاءاتها تختلف بين سياق وآخر، وتتوقف نتائجها المرجوَّة على عواملَ مختلفة. لذا يقدِّم التقرير نموذجًا لقياس مدى نُضج البوت وتطوُّر قدراته، ومقارنة فائدته العملية حاليًا بالمأمول من تطوره مستقبلًا. ويتكوَّن هذا النموذجُ من قياس مدى قدرة البوت على كلٍّ من:

- **الوعي**: أي قدرة البوت على إيجاد الحدِّ الأدنى من المحتويات وتخزينها وتفسيرها. وإن تطورَ هذه القدرة يعني تمكُّنَ البوت في المستقبل من معالجة اللغة الإنسانية الطبيعية، وتطور فهمه لأنماط الحديث البشري، بالتفريق بين الدَّلالات الدقيقة لمعاني الكلمات، وربما المعاني المجازية.



- **التقرير:** أي قدرة البوت على تصنيف المحتوى والبيانات الأخرى إلى فئات لها معنًى، وهذا يسهِّل عملية اتخاذ القرار بشأن هذه البيانات أو المستخدمين آليًّا. وعلى الرغم من نُضج هذه القدرة إلى حدٍّ كبير، لا يزال التعلُّم الآلي يواجه أخطاءً مختلفة ناتجة عن الخطأ في التصنيف. وهذا يسترعي ضرورةَ الحذر من منحِ البوتات الثقةَ الكاملة في اتخاذ القرارات. وتُنبئ الكثير من المقابلات التي أجراها الباحثون عن استمرار الصراع في المستقبل على تطوير قدرة الحكومات على اكتشاف البوتات، وقدرة مديري هذه البوتات على التخفِّي. ويُعَدُّ العامل البشري جزءًا حيويًّا في هذا الصراع، وقد حاول تنظيمُ الجهاز السيبيري لداعش رِشوةَ أحد موظفي الشركات المكلَّفة منعَ الترول والبوتات الخاصَّة بالتنظيم، من بناء حسابات على تويتر.
- **الفعل:** أي قدرة البرنامج على القيام بأفعال بشرية في العالم الواقعي أو الافتراضي، كإرسال طلب صداقة، أو الردِّ على تعليق. وقد تطورت تقنيةُ البوتات تطورًا كبيرًا في هذا الاتجاه، إلا أن هذه البرامجَ لن تكونَ قادرةً على إجراء مناقشات مطوَّلة مع المستخدم البشري دون إثارة شكوك، وهذا يؤكِّد ضرورةَ استمرار المدير البشري في مراقبة أدائها، والتدخل قدرَ الإمكان. ويتوقَّع الباحثون أن الجيل القادم من البوتات سيتجاوز جيلَ الرسائل الحالي إلى التلاعب بالمقاطع المرئية والصوتية. وقد تمكّن الباحثون في جامعة واشنطن من معالجة بعض المقاطع المرئية، ودمج بعض المقاطع، ووضع بعض الكلمات على لسان بعض الأشخاص.

المخاطر القانونية

إن مخاطر استخدام البوتات كثيرة، وتختلف من بوت إلى آخر، بحسَب نوعه وهدفه والمشغِّل له، وإذا كان البرنامج يُستخدَم في بلدٍ ما فمن المرجَّح أن عواقبه ستتجاوز الحدود. وتعَدُّ البوتات التي تنتهك الخصوصية والسرِّية وترابط المعلومات وتوافرها تهديدًا حقيقيًّا، مما يمكِّن الحكومة الأمريكية من بناء سياسة لمواجهة أخطارها، ووضع قواعدَ مختلفة قد تُحتذى في بلدان أخرى، مع ضعف احتمال صيرورة السياسة الأمريكية عُرفًا متَّبعًا. ويمكن دحضُ مخاطر جمع المعلومات من قِبَل البوتات بواسطة الوسائل المستعملة فعليًّا. ويؤكِّد التقرير أن الحكومة الأمريكية لن تلجأَ إلى استخدام البوتات في تحقيق أهداف يمكن الوصولُ إليها دون استخدامها، ولن تلجأَ إلى نشر أخبار معينة أو التخفِّي وراء قناع شخصية بشرية. لذا سيكون من الأوفق أن تشارك الحكومة الأمريكية منصَّات الرسائل؛ لتفعيل شروط الاستخدام المعتمَدة قانونيًّا؛ للتقليل من تأثير البوتات.

ومن المعضلات القانونية ما يأتي:

- **فقرة (حرية التعبير)** في التعديل الأول من الدستور: تنصُّ على **ضمان حرية التعبير، ومنع الحكومة من اختراقها**، وتمتدُّ هذه الحرية إلى التعبير السياسي

دون أن تشملَ الخطاب المحرِّض على الكراهية والعنف مع أقلِّيات أو أشخاص محدَّدين. وبسبب خفاء الحدود الفارقة بين المحتويين فقد يُعدُّ المحتوى الذي يبثُّه تنظيم داعش الإرهابي بما يتضمَّنه من مشاهدَ عنيفة ودموية ضمنَ حدود حرية التعبير السياسي. فإذا تمتَّع بعض المحتوى بالحماية وجبَ على الحكومة الأمريكية اتِّباعُ الإجراءات القانونية للتعامل معه، كإصدار أمرٍ من المحكمة. وكذلك إن أرادت الحكومةُ استخدام البوتات لحذف محتوًى معين، فسيكون عليها أن تتَّبعَ الإجراءات نفسها. إلا أن للحكومة إجبارَ المنصَّات الرَّقْمية على حذف محتوًى معين، فغالبًا ما تحتوي شروطُ الاستخدام في هذه المنصَّات على منع الترويج للدعاية الإرهابية، حتى لو كانت خاضعةً لحرية التعبير، وتتيح هذه الشروطُ للمستخدمين أن يبلِّغوا عن مثل هذا المحتوى لحذفه. وقد أسست الحكومةُ البريطانية وَحدةَ إحالة لمكافحة التطرف تمكَّنت من حذف ألفَي مادَّة في الأسبوع الواحد، وهو المثال الذي احتذاه الاتحادُ الأوروبي في 2015م، وتمكَّنت هذه الوَحدة من معالجة ما يزيد على 11 ألف رسالة.

- **فقرة (التأسيس)** في التعديل الأول للدستور: **تنصُّ على منع الحكومة الأمريكية من التمييز والمفاضلة بين الأديان في التعامل.** وقد تطرح هذه الفقرةُ أسئلة عند اختيار الحكومة استخدام البوتات لاستهداف أتباعِ دين معيَّن، وتشمل هذه المخاطرُ بوتاتِ التأثير والحصاد والأقنعة والتحرش. وستُعتمَد المساءلة القانونية إذا ما كان تصميمُ البوتات وتوظيفها يستهدفان المستخدمين الذين يتَّبعون جماعة دينية معينة، أو كلمات محدَّدة. ولتجاوز هذه المخاطر من الممكن استهدافُ الأشخاص الذين يعيشون في الخارج؛ لأنهم على الأرجح لن يتخذوا إجراءات تجاه الحكومة الأمريكية. ولكن يجب على المطوِّرين أن يكونوا حذرين تجاه الكلمات المفتاحية التي يبحثون عنها؛ لئلَّا تكون متعلِّقةً بدين معين على نحو ضيق.
- **الاستخبارات وتطبيق القانون:** قد يكون لبعض البوتات أهميةٌ لتطبيق القانون والعمليات الاستخباراتية، ولا سيما «بوتات الحصاد». وتكون محاولتها للولوج إلى المعلومات غير المتاحة علنًا يجعلها خاضعةً لقيود وعمليات قانونية معينة، منها: قانون الخصوصية، وقانون خصوصية الاتصالات الإلكترونية، وملحق الاتصالات بالقوانين التطبيقية، وقانون تخزين الاتصالات، وقانون الرقابة على المعلومات الاستخباراتية الخارجية، وغيرها. ويجب على الجهة التي توظِّف البوتات لجمع المعلومات أو في العمليات الاستخباراتية أن تتيقَّن انتفاءَ انتهاكات هذه القوانين.
- **قانون سميث- مونت:** هو قانون التبادل التعليمي والمعلوماتي لسنة 1948م، وينصُّ على السماح للحكومة الأمريكية أو مجلس إذاعة الحكام أن تقيمَ حمَلات للتأثير في الرأي العام في الخارج، لكنَّه يضع قيودًا على هذه الحمَلات في الداخل. ويحدُّ هذا القانون من الموادِّ الإعلامية التي تنتجها الحكومة، إلا أن تحديث القانون في عام 2012م أجاز للحكومة والمجلس المذكور إتاحةَ الحمَلات التي تستهدف الجمهور الأمريكي في الخارج. ولا بدَّ عند استخدام البوتات في تلك الحمَلات من مراجعة القانون، والتحقُّق من الجمهور المستهدف في تلك الحمَلات.

القيود الأخلاقية

ذكر التقريرُ عددًا من القيود الأخلاقية التي تختلف كثيرًا عن القيود القانونية، لكنَّها تفتقد إلى وسيلة التنفيذ. وعند القيام بعمليات مكافحة التطرف العنيف أو الإرهاب تعتمد الحكومةُ الأمريكية على منصَّات التواصل الاجتماعي التي تمتلكها شركاتٌ خاصة. وهذه الشركاتُ لها مصالحها الخاصة التي قد لا تتفق مع مصالح الحكومة وأهدافها، وقد يُخلُّ استخدام البوتات في هذه المنصَّات بحيادها، وإن شروط الاستخدام تختلف بين منصَّة وأخرى. ويؤكد الباحثون ضرورةَ أخذ هذه العوامل بالحُسبان حتى لا تتضرَّرَ هذه الشركات التي تعدُّ جزءًا رئيسًا من الاقتصاد الوطني.

وتؤكِّد المقابلات التي أجراها الباحثون أن الشفافية مطلبٌ أخلاقي وعملي عند تفعيل استخدام البوتات، فكثيرٌ من الأمريكيين وغيرهم لا يتوقعون أن الحكومة الأمريكية تستخدم البوتات وغيرها من تقنيات التواصل لتحقيق أهداف سياسية، أو لتقديم موادَّ دعائية. فمن الضروري الحذرُ عند التعامل مع هذه الموادِّ، إذ إن سوء استخدامها بالتلاعب بالمعلومات أو التضليل المتعمَّد قد يأتي بالضرر على سُمعة الحكومة الأمريكية والثقافة السياسية التي تضع توقعات معينة لأدائها. كذلك قد يؤدِّي إلى تراجع الثقة بشبكة الإنترنت بوصفها مساحةً آمنة لتبادل المعلومات، وسيكون لذلك عواقبُ اقتصادية وتجارية وسياسية على السياسة الأمريكية التي تدعم تعزيزَ المساحات الآمنة في الإنترنت. لذا، يدعو الباحثون الحكومة الأمريكية

لإصدار بيان مبادئ عام يوضِّح نوع البوتات التي تستخدمها، والطرق المختلفة التي توظفها بها، وذلك يمكِّن الجمهورَ من تفهُّم ما تقوم به الحكومة، وقد يكون من المفيد أيضًا أن تُنشئَ الحكومة مدوَّنات الاستخدام المسؤول للبوتات، سواء داخل الحكومة أو خارجها.

إن المخاطر الأخلاقية لاستخدام البوتات تختلف بين مؤسسة وأخرى، فوِزارة الخارجية تنهض بمسؤوليات كثيرة تتجاوز عمليات مكافحة التطرف والإرهاب إلى تعزيز المصالح الاقتصادية، ودعم حرية الإنترنت وحقوق الإنسان في العالم، وقد يتضمَّن توظيفُها للبوتات مخاطرَ أعلى، وقد ينتج عن ذلك ما يقوِّض المصالح الأمريكية. أما المؤسساتُ ذات المهام الضيقة أو غير الاستشارية كوِزارة الأمن الداخلي فإن مخاطرها أقلُّ؛ نظرًا لتخصصها في تأمين الإنترنت.

التطوير والتقويم

بعد إيضاح مدى أهمية استخدام الحكومة الأمريكية للبوتات في مكافحة التطرف العنيف والإرهاب، وإمكانية ذلك، تناول التقريرُ التطويرَ الفعلي لبوتات مكافحة الجماعات الإرهابية كتنظيم داعش الإرهابي وغيره. ويسبق ذلك تطويرُ مفاهيم هذه العملية وتقويمها، والمقصودُ بهذه المفاهيم هو الأسُس العامة للبرامج، فالبرنامج الذي يحاول بفاعلية أن يقدِّمَ الموارد الضرورية للأفراد والجماعات التي تواجه خطر التحوُّل إلى الأصولية يختلف عن برنامج البوت الذي يستهدف مكافحةَ نشر المعلومات الزائفة من قِبَل خصوم الولايات المتحدة. وقد بيَّن التقرير أن **معايير تقويم هذه المفاهيم تتمثَّل في الآتي:**

1. **الجدوى التقنية للبوت** بوصفه متطورًا تقنيًا، ولديه من القدرات التفاعلية ما يجعله أهلًا للاستخدام.
2. **المخاطر على مستخدمي البوتات**، وتشمل المخاطرَ الاجتماعية والمادِّية، ومخاطرَ الخصوصية.
3. **المخاطر المحتمَلة على مطوِّري البوتات أو موظَّفيها**، وتتمثل في مخاطر الانكشاف، أو تعرُّضهم لمشكلات قانونية.
4. **حجم التأثير**، كالقُدرة على التفاعل مع القدر الأكبر من جمهور المستخدمين، وجَودة التفاعل.
5. **التراكيب أو التعقُّد**، ويشمل القدرة على تنسيق التفاعل والتزامن والتشغيل مع برامجَ أخرى.

ويستخلص الباحثون من هذه المعايير أحدَ عشرَ عاملًا بصيغة أسئلة لتحديد نوع عملية توظيف البوتات، مثل: مَن القائمُ على عملية التوظيف؟ وأين يمكنُ توظيفها؟ وما إستراتيجيةُ الاتصالات التي سيستخدمها البوت؟ ومتى يمكنُ تفعيل البوت؟ وكيف تعملُ البوتات؟ وعلى أيِّ مستوًى من التشغيل يمكن كشفُ البوت؟

ولإيضاح تفاصيل عملية التقويم المتصلة بالمستخدمين، فإن كان المستهدف من تشغيل البوتات هو الجمهور العالمي، فقد تكون الجدوى التقنية أوسع، مع وجود مخاطرَ عالية على مطوِّر البوت. أما إن كان المستهدف هو الجمهور الأمريكي، فالجدوى التقنية أقل، والمخاطر على مطوِّر التقنية أعلى. وأما إن كان

المستهدف المواطنين المقيمين في البلاد، فالجدوى التقنية أقل، والمخاطر على المطوِّر أقل بكثير. وإن كان المستهدف هو الحسابات المعادية المؤكَّد تبعيتها لتنظيم داعش، فالجدوى التقنية أعلى، والمخاطر غير قائمة. أما الجدوى التقنية لتوظيف البوتات مع الأشخاص المعرَّضين لخطر التحوُّل إلى الأصولية فهي أعلى، وكذلك المخاطر الممكنة على مطوِّري البوت. وترتفع درجة الجدوى التقنية عند استهداف البوتات لخصوم داعش، وتقلُّ المخاطر على مطوِّري البرنامج.

ويشير الباحثون إلى إمكانية توظيف الذكاء الاصطناعي والتعلُّم العميق لتعزيز عملية التقويم، فبعض البوتات تعتمد على إدارة بشرية، وتتمتَّع برامجُ أخرى باستقلالية كاملة في الحركة، بناءً على توظيف الذكاء الاصطناعي والتعلُّم العميق، وبمعالجة عدد كبير من البيانات عبر الدالَّات الحسابية المعروفة بالخُوارِزميات.

إن البرامج التي تعتمد على الذكاء الاصطناعي تُتيح الحصولَ على أفكار وآراء قد تَخفى على العين البشرية المجرَّدة. ويمكنها أن تعزِّزَ قدرة الفاعل البشري على التخفِّي، وعلى الدخول في تفاعلات مباشرة مع المستخدمين. وأهمُّ من هذا أنها قد تعزِّز قدرة البوت على التخفِّي.

وفي الاعتماد على الذكاء الاصطناعي مخاطرُ عديدة، أهمها: أن البرامج قد تتصرَّف بعيدًا عن النصِّ الموضوع لها، وأنها قد تتورَّط في مسائلَ أخلاقية أو قانونية، وربما تصرَّفت على نحو غير متوقَّع، فتصبح عُرضةً للانكشاف. ووَفقًا لتوصية أحد خبراء تقنية البوتات: من الضروريِّ أن تبقى هذه البرامجُ مقيَّدةً تحت الرقابة البشرية؛ لئلَّا ينتهيَ أحد البرامج المستخدمة في مكافحة الأصولية إلى أن يتحوَّل هو نفسه إلى برنامج أصولي.

بناءً على هذا التقويم، يستنتج الباحثون أن أفضل البوتات التي تستهدفُ التأثير في الجمهور، ونشر الأخبار هي «بوتات المقابلة»؛ بسبب قلَّة المخاطر الأخلاقية والقانونية التي تواجهها، والتقنية المتاحة لاستخدامها. أما البوتات التي تستهدفُ تقويض الشبكات المتطرفة والحدَّ من تأثيرها، فهي «البوتات الكاشفة أو الفاضحة»؛ بسبب الجدوى التقنية من استخدامها، وضعف مخاطرها على المطوِّرين والجمهور العام من مستخدمي منصَّات التواصل الاجتماعي. أما البوتات التي توظَّف لجمع المعلومات السرِّية فهي «بوتات الحصاد»، وهي أكثرُ جدوًى من البوتات المصمَّمة للاصطياد.

وقد عرض التقرير نموذجًا لبناء مفهوم عملية استخدام بوتات المقابلة يسعى إلى تقديم الموارد الكافية للمواطنين المعرَّضين لخطر التحوُّل إلى الأصولية. هذا البوت يتمتَّع بالشفافية، ويتفاعل معه المستخدمون بواسطة الإعلان، ويشارك في عملية التشغيل مديرٌ بشري، ويولي أهميةً لتقليل المخاطر على المطوِّرين، وعلى الجمهور المستخدم لمنصَّات التواصل الاجتماعي، ويتفاعل معه المستخدمُ دون التحكُّم في بياناته الخاصة، والمستخدمون هم من الأشخاص البالغين من غير مواطني الولايات المتحدة.

توصيات ومقترحات

خصَّص الباحثون القسم الأخير من التقرير لتقديم عددٍ من التوصيات للجهات المختصَّة في الحكومة الأمريكية، عن تطوير البوتات، وتفعيل استخدامها، ومعالجة القضايا الأخلاقية والقانونية المتعلِّقة بها عند مكافحة التطرف. وبيَّن الباحثون أن عدَّة قضايا ينبغي للمؤسسات الأمريكية المعنية أن تهتمَّ بها عند تطوير برامج البوتات، وتتجلَّى في الآتي:

1. الإفادة من التطوير التجاري لتقنية البوت، مع التقدُّم الواضح الذي يُحدثه الاستثمار في هذه الصناعة.
2. تطوير البوتات بناءً على البيئة التي ستوظَّف فيها، ومراعاة وسائل المنصَّة التي ستُطلَق فيها، وكيفية تفاعلها مع المستخدمين، والرقابة الحكومية على المستخدمين في بعض البلدان. ومن شأن هذه العوامل أن تزيدَ من الثقة في العملية، وأن تقلِّلَ المخاطر التي قد تحدث للمطوِّرين والمستخدمين على السواء.
3. الانتباه إلى خصائص الشبكات التي يسعى المستخدمون للتفاعل معها، كوجود أصدقاءَ للمستخدمين في هذه الشبكات، أو وجود اهتمامات مشتركة، أو كثافة التواصل الاجتماعي فيها. وغالبًا ما يشتبك المستخدمون بحسابات تصلهم بها اهتماماتٌ وأصدقاءُ مشتركون.

ويقترح الباحثون على الحكومة الأمريكية **عدَّة خطوات لتقليل المخاطر التشريعية والأخلاقية التي قد تنتج عن توظيف البوتات، منها:**

أ- ضرورة اهتمام المؤسسات المعنية بتحليل السوابق الدَّولية في استخدام برامج البوتات؛ وذلك لتجنُّب تطبيع أفعال الحكومات وتصرُّفاتها التي قد تؤدِّي إلى تهديد الأمن السيبراني، بواسطة التدخُّل في السرِّية أو تكامل المعلومات على الإنترنت وإتاحتها.

ب- مراعاة القضايا المتعلِّقة بالنصوص والمسائل القانونية؛ بجعل عملية توظيف البوتات على نطاق ضيِّق من المستخدمين في الخارج، مع تجنُّب استهداف المستخدمين الذين ينتمون إلى طائفة دينية معينة. وضرورة بناء جدار حماية عندما يكون الوضع ملائمًا بين عدد من برامج البوتات، وجهات الاستخبارات، وإنفاذ القانون، والشركاء الدَّوليين.

ت- ضرورة الحصول على إذن الشركات قبل توظيف البوتات واستخدامها على منصَّات التواصل الاجتماعي.

ث- ضرورة الشفافية قدرَ الإمكان في عمليات استخدام حكومة الولايات المتحدة للبوتات، وأن تكونَ في حدود معينة مدروسة لتلافي العواقب غير الحميدة.

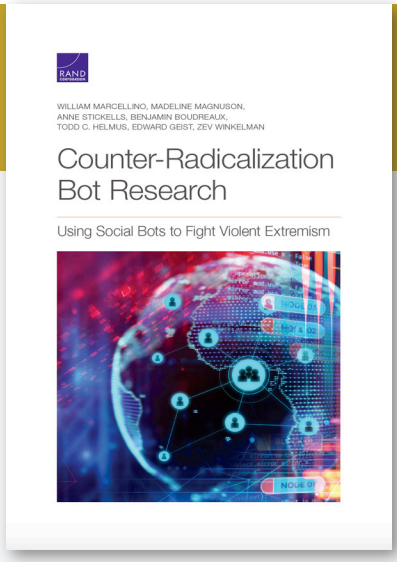
ج- ضرورة إجراء مراجعة قانونية للبوتات المستخدمة بتعاون داخلي بين المؤسسات؛ وذلك لتطوير مبادئ عملها، وإنشاء مدوَّنة لذلك.

خاتمة التقرير

يختتم الباحثون التقرير بالقول: إن دراسة وضع استخدام البوتات يؤكِّد أنها أداةٌ عملية في مكافحة التطرف العنيف والإرهاب، إلا أن توظيفها سيكون مقيَّدًا بكثير من العوامل القانونية والأخلاقية والعملية، وهذا ما يوجب دائمًا وجودَ العامل البشري. وينبغي لصُنَّاع القرار أن يوازنوا بين المنافع المتوقَّعة لتوظيف البرامج، والمخاطر المتضمَّنة في البرامج التي تعمل ذاتيًا. وكذلك ينبغي للحكومة الأمريكية أن تعزِّزَ تقنيات اكتشاف البوتات؛ مما يصعِّب على الخصوم شنَّ حمَلات خداع وتضليل، ونشر معلومات خاطئة بواسطة البوتات، مع مراعاة إدراك السياق الثقافي والاجتماعي عند إنشاء البوتات.

وقد تناول التقريرُ أحدَ التطورات الضخمة في عالم التقنيات السيبرانية، وهي البوتات، وقوَّم إمكانية استخدامها في مكافحة التطرف العنيف والإرهاب. وبحث في القيود القانونية والأخلاقية التي ينبغي مراعاتُها عند توظيف الحكومات للبوتات في عمليات مكافحة التطرف. إلا أن التقرير على الرغم من أهمية موضوعه، واعتماده على بحث مَيداني واسع، يتَّسم بالتوسُّع في الجانب التقني، وذلك كان حائلًا دون التفصيل في كيفية توظيف البوتات في مكافحة التطرف والإرهاب، ولا سيَّما في شبكة الإنترنت. إلا أن إشاراتٍ ضئيلةً إلى كيفية استخدام التنظيمات المتطرفة والإرهابية للبوتات المختلفة وردت في التقرير.

وقد ذكر التقريرُ في بدايته أن التنظيمات الإرهابية كتنظيم القاعدة وداعش وظَّفت تقنيات البوت وغيرها في التجنيد والدعاية، ولم يقدِّم أمثلة أو إحصاءات أو قياسًا لمدى نجاح هذه العمليات، وما آلت إليه بعد انحسار التنظيمين في الشرق الأوسط على وجه التحديد. مما يجعل هذا التقريرَ غير متوازن من حيثُ الموضوع، لكنَّه مفيد للمؤسسات المشاركة في مكافحة التطرف؛ بما بيَّنه من حقيقة هذه المكافحة بجوانبها السياسية والأمنية والاقتصادية والثقافية المركَّبة.



أبحاث بوتات مكافحة التطرف

توظيف البوتات في محاربة التطرف العنيف

COUNTER-RADICALIZATION BOT RESEARCH

USING SOCIAL BOTS TO FIGHT VIOLENT EXTREMISM

الصادر عن

مؤسسة RAND ، سانتا مونيكا ، كاليفورنيا.

2020


التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

التحالف الإسلامي العسكري لمحاربة الإرهاب

ISLAMIC MILITARY COUNTER TERRORISM COALITION