

الجيش الإلكترونيّ.. ساحة حربٍ من نوعٍ آخر



تحقيق: أحمد شعيتو

هي ساحة حرب ومواجهة من نوع آخر، توازي بمفعولها الحروب الأمنيّة والعسكريّة والاقتصاديّة، وتتزامن معها، وتستمرّ حتى بعد توقّف إطلاق النار. ميدانها شبكة الإنترنت ومواقع التواصل الاجتماعيّ، ينشط فيها ما يسمّى بالجيش الإلكترونيّ وقراصنة الإنترنت. هي حرب "سيبرانيّة" باتت تتنامى أدوارها وخطورتها ومحاولات تأثيرها في بيئتنا بطرق مختلفة. ففي ساحة استهداف الأحرار والمقاومين وبيئتهم، أصبح دور الجيش الإلكترونيّ خطيراً؛ لذا، نسلط الضوء عليها في هذا المقال، بشكلٍ علميٍّ، بهدف التوعية على أُسس عملها وطرق مواجهتها.

تتصاعد في الآونة الأخيرة وتيرة الحرب السيبرانية بين الدول والاستخبارات العالمية، ولا تقل أهمية هذه الحرب عن الحروب التقليدية، ولهذا السبب تخصص لها أموالاً وموازنات كبرى.

تستخدم ساحة الشرفاء التقنيّات وتُبدع بها لإيصال الكلمة الصادقة، بينما الساحة المعادية تستخدم كلّ الوسائل والتطوّر التقنيّ بأسلوب خبيث لبثّ السموم والأكاذيب عبر جيوش إلكترونيّة، هي عبارة عن مجموعات مدرّبة في ساحة مواقع التواصل، وعبر حسابات وهميّة و"روبوتات"، وهذه كلّها تُستخدم بقوة ضدّ ساحتنا. كما إنّ المواقع الإلكترونيّة الكاذبة والقنوات المضلّلة، تحاول أن توجي بأنّ الجيوش الإلكترونيّة تستخدم من قِبَل بيئة المقاومة وأهلها والوطنيين وأحرار الأمّة، لكي تبرئ ساحتها من الأضاليل.

الهدف: إيقاع الفتنة

في كلمة له حول التطوّرات في حزيران عام 2020م، تطرّق الأمين العام لحزب الله سماحة السيّد حسن نصر الله (حفظه الله) إلى هذه المخاطر، فقال: "ثمّة في لبنان حالة تفلّست وانحطاط أخلاقيّ، وإسفاف وعدم انضباط، سواء في الشارع، أم عبر مواقع التواصل الاجتماعيّ، وأحياناً في وسائل الإعلام المرئيّة والمسموعة والمكتوبة، والأخطر من ذلك كلّّه وجود صعوبة في ضبط هذا الأمر بشكلٍ كامل. مسؤوليّتنا جميعاً؛ (...) وكلّ من لديه إحساس بالمسؤوليّة، أن لا نسمح لبلدنا أن ينجرّ إلى الفوضى وإلى الفتنة. وهذا الأمر سيستمرّ؛ إذ نشهده يوميّاً عبر مواقع التواصل".

وأضاف: "طالما أنّ الإعلام غير منضبط، ومواقع التواصل الاجتماعيّ غير منضبطة، فإنّ الانحطاط الأخلاقيّ والاختراقات الأمنيّة والإسفاف والعيث، ستبقى موجودة في البلد. بمعنى أنّ الجيوش الإلكترونيّة، الإسرائيليّة وغير الإسرائيليّة، والتي تريد أن تعمّ الفتنة هذا البلد، هي جاهزة كلّ يوم لأن تطلق

السباب والشتم، وإهانة رموز ومقدسات كل المسلمين والمسيحيين، وكل القوى السياسيّة، للإيقاع فيما بينهم".

مخاطرها المتنامية

ثمّة الكثير من المخاطر المتصاعدة في الآونة الأخيرة للجيش الإلكترونيّ المعادية لساحتنا، منها:

1- إثارة الشحن والبعضاء والتفرقة من أجل إضعاف الساحة. وقد تتطوّر مخاطرها من البغض والحقد من ردود فرديّة إلى ردود جماعيّة، وصولاً إلى فتن داخليّة، بل إلى حروب أهليّة.

2- الإيحاء بوجود رأي عامّ مؤيّد أو معارض لفكرة أو لشخص أو قرار، وذلك لجذب أكبر عدد من غير المتعمّقين بتلك الأمور أو الإجراء.

3- إثارة ضغوط نفسيّة لتوهين الإرادة والقدرة على الصمود.

4- إثارة البلبلة عبر تحريك نقاش ما في موضوع حسّاس يثير ردود فعل سلبية.

5- محاولة تبخيس أيّ إنجاز لساحة المقاومة.

6- تشويه الصورة؛ وهو من أخطر الأهداف التي تعمل عليها الجيوش الإلكترونية، حيث يتمّ تحميل الشرفاء والوطنيين الموبقات ومسؤولية أيّ فشل أو خطر أو تراجع أو خيبة.

7- شتم الرموز الدينية لإثارة الفتن المذهبية والطائفية.

8- الدعاية السياسية والتطويل لجهات معينة.

9- تخويف المواطنين.

تضليل الرأي العامّ

تحدّث مدير التواصل الاجتماعيّ في قناة المنار، الأستاذ حسن نور الدين، لمجلة بقية ا، حول أسس عمل الجيوش الإلكترونية، أو الذباب الإلكترونيّ، وطرق التحقّق من كذبها وخداعها. وقال: "في ظلّ فوضى المعلومات على المنصّات الرقمية، لا بدّ من اعتماد أكثر من منهجية للتحقّق من عمليّات التلاعب في المحتوى؛ لأنّ الأمر غير مقتصر على المعلومة الزائفة، بل يتعدّاه إلى التضليل من خلال السياق المغلوّط.

وتظهر خطورة الأمر في سرعة انتشار هذه المعلومات على منصّات التواصل الاجتماعيّ، مضافاً إلى سهولة

القيام بهذه الأنشطة من تلاعب وتضليل. ولا بدّ من فهم السياق لتحديد الدوافع من وراء نشر هذه المعلومات، والتي تنوّع ما بين الدافع الماليّ والسياسيّ، ناهيك عن الدافع النفسيّ والاجتماعيّ".

وأشار إلى أنّ "الأساليب المعتمدة في عمليّات التضليل ونشر المعلومات المغلوطة تتعدّد، ولكنّ الهدف الأساسيّ هو إقناع أوسع شريحة ممكنة، من خلال تشكيل رأي عامّ حول الموضوع المطروح، وتضليل أكبر قدر ممكن من المتابعين، وتحويلهم إلى جنود داعمين للقضيّة، ما يساعد في عمليّة الانتشار".

أضاف نور الدين: "يجب فهم كميّة عمل أبواق التضخيم لتحديد مدى قدرة الذباب الإلكترونيّ على نشر قضيّة ما وتحويلها إلى قضيّة رأي عام. بغضّ النظر عمّا إذا كانت سلبية أم إيجابية، حيث تبدأ أبواق التضخيم من خلال بعض الحسابات التابعة لمجموعة ذباب إلكترونيّ بالعمل على نشر قضيّة ما عبر شبكات مغلقة أو شبه مغلقة، ما تلبث أن تبدأ مشاركتها باقي الحسابات على مواقع التواصل الاجتماعيّ. والعدد الأكبر من هذه الحسابات يكون على ارتباط بالمجموعة نفسها، وسرعان ما تنتشر لتصبح تمثّل قضيّة رأي عام. من هنا، يظهر أنّ الدعامة الأساسيّة لأيّ ذباب إلكترونيّ؛ هو الحسابات المنصوية تحت هذه المجموعات. وتكمن فعاليّة الانتشار في مدى تأثير هذه الحسابات بالشبكات الخاصّة (البيئة المحيطة) لكلّ حساب".

الحسابات: نوعها ودورها

بحسب نور الدين، يوجد ثلاثة أنواع من الحسابات:

2- الحسابات البشريّة

3- حسابات Cyborg (مزيج بين الآليّ والبشريّ).

الحساب الآليّ هو تطبيق برمجيّ يقوم بمهام محدّدة مسبقاً من قِبل عناصر بشريّة. وتختلف المهام حسب دوافع المشغّل البشريّ: إمّا أن تكون حميدة أو خبيثة. والهدف الرئيس منها هو إثبات وجود قاعدة شعبيّة تدعم قضيّة ما. وعلى الرغم من أهميّة الحسابات البشريّة ودورها الفاعل، إلا أن معظم مجموعات الذباب الإلكترونيّ تفضّل العمل على الحسابات الآليّة بسبب الكلفة المتدنّية للموازنة التشغيليّة مقارنةً بالحسابات البشريّة.

بعض أنواع الحسابات الآليّة:

1- الحسابات التي تعتمد الجدولة: يتم جدولة النشر من قبل عنصر بشريّ على هذه الحسابات بأوقات محدّدة.

2- الحسابات التي تعتمد على المراقبة: يتمّ تحديد حسابات وصفحات معيّنة، وتقوم هذه الحسابات بأخذ المحتوى منها وإعادة نشره.

3- الحسابات التي تعتمد على الترويج: المشاركة من حسابات محدّدة لدعمها، ووضع إعجاب "Like"، وإعادة التغريد "retweet".

كيفية التحقّق من الحسابات الآليّة

أوّلًا: يجب التأكيد على أنّ عمليّة التحقّق من الحسابات تتطلّب مجهودًا خاصًّا يتجاوز تدريب "علم الأزرار" واستخدام الأدوات التقنيّة، بل يجب التدرّب على كيفية فهم البيانات وارتباطها بالسياق العام لاستخلاص أفضل النتائج.

ثانيًا: كما يجب توفير الاستعداد والرغبة لقراءة مئات التغريدات، والغوص في منصّات التواصل الاجتماعيّ.

ثمّة مجموعة من الخطوات يمكن اتّباعها لتحديد السلوك المشبوه للحسابات على وسائل التواصل:

1- المتابعة الدقيقة للحساب المشبوه.

2- استخدام الأدوات المتوفّرة في الكشف على الحساب.

عناصر التحقّق من الحساب

ما هي العناصر التي يجب الالتفات إليها عند التحقّق من الحسابات؟

1- الهوية الخاصّة للحساب: كلّ حساب له هويّة خاصّة. وعادةً، يتمّ إغفال تحديثها في الحسابات الآليّة بخلاف الحسابات البشريّة.

بدايةً، يجب مراجعة اسم المستخدم (username)، حيث يتمّ توليد معظم الحسابات الآليّة بشكل آليّ (تتوفّر برامج لخلق الشخصيات)، ويعتمد نمطاً محدداً في التسمية (username)، كاعتماد اسم من أرقام أو اسم يتبعه عدد محدّد من الأرقام، أو اسم عشوائيّ من عدد محدّد من الأحرف أو الأرقام. ومن خلال بحثٍ بسيطٍ عن النمط المعتمد، يمكن أن يظهر لنا باقي الحسابات المشابهة. في حال كان اسم المستخدم حقيقياً، نبحث عن البصمة الإلكترونيّة لهذا الاسم، ومطابقتها مع باقي الحسابات التي تحمل الاسم نفسه.

2- الصورة الشخصيّة للبروفيل: وهي خطوة أساسيّة في عملية التحقّق؛ لأنّ معظم الحسابات البشريّة تعتمد إلى تعديل الصورة من فترة إلى أخرى، وهذا ما لا يتوفّر في الحسابات الآليّة، بحيث تكون وهميّة أو مسروقة. يمكننا من خلال استخدام أدوات البحث العكسيّ للصور التعرّف على صاحب الصورة الحقيقيّ. تتوفر بعض الأدوات الخاصّة، والتي تعتمد على مجموعة من المعايير لتحديد مدى آليّة الحساب أو بشريّته.

3- نشاط الحساب: يجب مقارنة عمر الحساب مع نشاطه، وتحديد الفترات الزمنية التي مرت عليه منذ إنشائه. فيُعدّ جدول تفصيليّ بكلّ حركة الحساب، تتضمّن فترات ثباته ونشاطه. مضافاً إلى رصد معدّلات التغريدات اليومية وتوزّعها الزمنيّ، لإظهار أيّ أنماط مشبوهة في التغريدات؛ إذ إنّ الحسابات الآليّة تعتمد نمطاً منتظماً من التغريد من ناحية الوقت وارتباطه بالأحداث التي تتطلّب حملات محدّدة. وأخيراً، البحث في التغريدات المحذوفة باستخدام أدوات خاصّة.

4- علاقات الحساب: هي أحد العناصر التي تساعد على تحديد تبعيّة الحساب لمجموعة محدّدة من الذباب الإلكترونيّ. فمن خلال مراقبة أعداد المتابعين ومعدّل زيادتهم، مضافاً إلى تحديد نمط التفاعل مع الحسابات الأخرى، يكمن معرفة: لمن تعود هذه الحسابات؟ وهل لها أيّ استهداف محدّد ومشارك؟ وهل يوجد لها نشاط موحّد وسلوك جماعيّ منسّق؟ وهل تعتمد أنماطاً مشابهة في المحتوى في حملات مختلفة؟ هذه الأسئلة وغيرها تساعدنا في تحديد نوع الحساب.

وهكذا، فلنكنّ بكامل الوعي والدقّة في التعامل مع مواقع التواصل الاجتماعيّ، ولنحذر من أيّ أمر مشبوه يثير الريبة والتساؤل.

المصدر: مجلة بقية ا