رصد وسائل التواصل الاجتماعيّ

عِبَرٌ لتحليلات وزارة الدفاع الأمريكية لوسائل التواصل الاجتماعي في المستقبل دعماً لعمليّات المعلومات

ويليام مارسيلينو (William Marcellino)، ميجان ل. سميث (Meagan L. Smith)، كريستوفر بول (Christopher Paul)، لورين سكرابالا (Lauren Skrabala)

RAND CORPORATION

NATIONAL DEFENSE RESEARCH INSTITUTE RAND

رصد وسائل التواصل الاجتماعيّ

عِبَرٌ لتحليلات وزارة الدفاع الأمريكية لوسائل التواصل الاجتماعي في المستقبل دعماً لعمليّات المعلومات

ويليام مارسيلينو (William Marcellino)، ميجان ل. سميث (Meagan L. Smith)، كريستوفر بول (Christopher Paul)، لورين سكرابالا (Lauren Skrabala)

للحصول على مزيدٍ من المعلومات حول هذا المنشور، الرجاء زيارة الموقع الإلكتروني:
www.rand.org/t/RR1742

تمّ نشر هذا البحث بواسطة مؤسسة RAND، سانتا مونيكا، كاليفورنيا
© حقوق الطبع والنشر لعام 2017 محفوظةٌ لصالح مؤسسة RAND
®RAND علامة تجارية مسجّلة.

صورة الغلاف: سديكوريت/فوتوليا *(sdecoret/Fotolia)*

حقوق الطبع والنشر الإلكترونيّ محدودة
هذه الوثيقة والعلامة (العلامات) التجارية الواردة فيها محميةٌ بموجب القانون. يتوفر هذا التمثيل للملكية الفكرية الخاصة بمؤسسة RAND للاستخدام لأغراضٍ غير تجاريةٍ حصرياً. يحظر النشر غير المصرَّح به لهذا المنشور عبر الإنترنت. يصرَّح بنسخ هذه الوثيقة للاستخدام الشخصيّ فقط، شريطة أن تظل مكتملةً دون إجراء أيّ تعديلٍ عليها. يلزم الحصول على تصريحٍ من مؤسسة RAND، لإعادة إنتاج أو إعادة استخدام أيٍّ من الوثائق البحثية الخاصة بنا، بأيّ شكلٍ كان، لأغراضٍ تجارية. للمزيد من المعلومات حول إعادة الطباعة تصاريح الربط على المواقع الإلكترونية، الرجاء زيارة صفحة التصاريح في موقعنا الإلكترونيّ: www.rand.org/pubs/permissions

مؤسسة RAND هي منظمةٌ بحثية تعمل على تطوير حلولٍ لتحدّيات السياسات العامة وللمساعدة في جعل المجتمعات في أنحاء العالم أكثر أمناً وأماناً، وأكثر صحةً وازدهاراً. مؤسسة RAND هي مؤسسةٌ غير ربحية، حيادية، وملتزمةٌ بالصالح العامّ.

لا تعكس منشورات مؤسسة RAND بالضرورة آراء عملاء ورعاة الأبحاث الذين يتعاملون معها.

ادعم مؤسسة RAND

تبرّع بمساهمةٍ خيريةٍ معفاةٍ من الضريبة على:
www.rand.org/giving/contribute

www.rand.org

تمهيد

تؤدي وسائل التواصل الاجتماعي دوراً مهمّاً ومتزايداً في عمليات المعلومات (Information Operations [IO]) العسكرية الأمريكية، لأن الناس من حول العالم، بما فيهم الشعوب المدنيّة، وحلفاء الولايات المتحدة، وخصوم الولايات المتحدة، يَسْتَخْدِمون منصات وسائل التواصل الاجتماعي من أجل تبادل المعلومات وإقناع الآخرين. منح النمو السريع لتكنولوجيات الاتصالات التي تدعم منصات وسائل التواصل الاجتماعي الخصوم غير الحكوميين ميزةً غير متماثلة، كالاستفادة من كلفة الدخول المنخفضة وخفّة الحركة التشغيلية النسبية التي يستطيعون بها، على عكس البيروقراطيات القائمة، الوصول إلى التكنولوجيات الجديدة واستخدامها. وبالتالي، في حين توجد أسبابٌ اضطراريّة مرتبطةٌ بالأمن القومي لنشر قدرةٍ على تحليل وسائل التواصل الاجتماعي، يتوجّب على وزارة الدفاع الأمريكية (U.S. Department of Defense [DoD]) القيام بذلك، مع مراعاة معايير قانونية وثقافية أمريكية وفي ظلّ ظروفٍ من عدم اليقين الكبير على حدّ سواء. في وسط اتجاهات التكنولوجيات والتواصل السريعة التطوّر، يظهر خطر يتمثّل باحتمال أن تستثمر وزارة الدفاع الأمريكية في قدرات ستصبح هالكة بعد فترةٍ وجيزةٍ أو تواجه تحدّيات أخرى في بناء قدرتها التحليليّة وتطبيقها بطريقةٍ فعّالةٍ وعمليّة.

يستكشف هذا التقرير هذه القضايا المُعقَّدة ويقدّم لوزارة الدفاع الأمريكية مجموعة من التوصيات لبناء قدرةٍ على تحليل وسائل التواصل الاجتماعي دعماً لعمليات المعلومات التي تعزّز بمهارةٍ وبشكلٍ ملائمٍ الأمن القومي. يجب أن يكون هذا التقرير ذا أهميّة خاصّة بالنسبة لمجموعة عمليات المعلومات المشتركة العسكرية الأمريكية. وبالنظر إلى الطبيعة المُلِحّة والتحدّيات التي يقترن بها تطوير هذه القدرة على حدّ سواء، وفي ضوء تقييم تم التفويض به من قِبَل الكونغرس، تحتاج وزارة الدفاع الأمريكية بشكلٍ واضحٍ إلى إجراء دراسةٍ استقصائيةٍ بحثيةٍ للدراسات السابقة القائمة حول تكنولوجيات تحليل وسائل التواصل الاجتماعي، والممارسات الفضلى، والقيود القانونية والأخلاقية المفروضة على تحليل وسائل التواصل الاجتماعي، وتقاطع عمليات المعلومات مع تحليلات بيانات

وسائل التواصل الاجتماعي.

أُجرِي هذا البحث برعاية مكتب الدعم التقنيّ لمكافحة الإرهاب (Combating Terrorism Technical Support Office) وفي مركز سياسات الدفاع والأمن الدوليّ التابع لمعهد أبحاث RAND للدفاع الوطني (International Security and Defense Policy Center of the RAND National Defense Research Institute)، وهو مركز بحوثٍ وتطويرٍ يعمل بتمويلٍ فيدراليّ، وبرعاية مكتب وزير الدفاع (Office of the Secretary of Defense)، وهيئة الأركان المشتركة (Joint Staff)، وقيادة المقاتلين الموحَّدّة (Unified Combatant Commands)، وقوات البحرية (Navy)، وقوات مشاة البحرية (Marine Corps)، ووكالات الدفاع (Defense Agencies)، ومجموعة استخبارات الدفاع (Defense Intelligence Community).

للمزيد من المعلومات حول مركز سياسات الدفاع والأمن الدولي التابع لمؤسسة RAND، الرجاء زيارة الموقع الإلكتروني www.rand.org/nsrd/ndri/centers/isdp أو الاتصال بالمدير (معلومات الاتصال متوفرة على الصفحة الإلكترونية).

المحتويات

تمهيد iii
الأشكال والجداول vii
الملخّص xi
الاختصارات xv

الفصل الأول
الحاجة إلى رصد وسائل التواصل الاجتماعي دعماً لعمليات معلومات وزارة الدفاع الأمريكية 1
غرض هذا التقرير ونطاقه 3
مقاربة الدراسة وأساليبها 5
هيكلية هذا التقرير 5

الفصل الثاني
كيف يمكن لتحليل وسائل التواصل الاجتماعي أن يدعم عمليات المعلومات 7
بيئة المعلومات والقدرات المرتبطة بالمعلومات 8
الاستخبارات 10
عمليّات دعم المعلومات العسكريّة 14
أمن العمليّات (OPSEC) والتضليل العسكري (MILDEC) 18
الشؤون العامّة 22
العمليّات المدنيّة–العسكريّة 23
انخراط القادة الرئيسيين 24
إطار عمل مرتكز إلى القدرات المرتبطة بالمعلومات (IRC) لبناء القدرة التحليليّة الخاصّة بوسائل التواصل الاجتماعي 24

الفصل الثالث
الأساليب التحليلية الخاصة بوسائل التواصل الاجتماعي لدعم عمليات المعلومات..... 27
محدوديّات وسائل التواصل الاجتماعي بوصفها مصدر بيانات 27
المفاهيم والأساليب الرئيسية في تحليل وسائل التواصل الاجتماعي 28
المقاربات لتحليل بيانات وسائل التواصل الاجتماعي 29

الفصل الرابع
السياق والاعتبارات لاستخدام تحليل وسائل التواصل الاجتماعي في عمليات المعلومات.... 51
القضايا القانونية 52
القانون الأمريكي الحالي وعمليات المعلومات..... 53
المخاوف المرتبطة بالباب 10 مقابل تلك المرتبطة بالباب 50 55
تطوير توجيهات واضحة في السياسات حول استخدام وزارة الدفاع الأمريكية (DoD)
لبيانات وسائل التواصل الاجتماعي..... 57
اعتبارات خاصّة: جمع المعلومات حول الأشخاص الأمريكيين..... 58
القضايا الأخلاقية 59
الاعتبارات المرتبطة بالبيانات والتكنولوجيا 61
الاعتبارات المرتبطة بالتدريب 62

الفصل الخامس
التوصيات 65
تطوير سياسات ولغة خاصّة بوزارة الدفاع الأمريكية (DoD) لتحليل وسائل التواصل
الاجتماعي..... 65
التوصيات للتنفيذ والدمج 68
التوصيات التقنية..... 69

المراجع 71

الأشكال والجداول

الأشكال

2.1. مكوّنات بيئة المعلومات 9
3.1. المجموعات الجامعة المؤيّدة والمعادية للدولة الإسلامية في العراق والشام (ISIL) على تويتر (Twitter) 34
3.2. الصدى اللغوي للدولة الإسلامية في العراق والشام (ISIL) في مصر، 2014 .. 42
3.3. الصدى اللغوي للإخوان المسلمين في مصر، 2014 43
3.4. الصور المُتبادَلة، بحسب النوع والموقع الجغرافي 50

الجداول

S.1. خارطة طريق للاستفادة من تحليل وسائل التواصل الاجتماعي لحملات عمليات معلومات وزارة الدفاع الأمريكية (DoD IO) xiv
2.1. أنواع القدرات المرتبطة بالمعلومات (IRC) وتعريفاتها 10
2.2. القدرات المرتبطة بالمعلومات (IRCs) والمقاربات المنهجية 25
3.1. مقاربات مختارة لتحليل بيانات وسائل التواصل الاجتماعي دعماً لحملات عمليات المعلومات (IO) 30
3.2. فئات العامة السنيّة في تحليل معارضة/دعم الدولة الإسلامية في العراق والشام (ISIL) على تويتر (Twitter) 37
3.3. كلمات مفتاحية نموذجية للدولة الإسلامية في العراق والشام (ISIL) والإخوان المسلمين، والترتيب في اختبار الرجحان اللوغاريثمي 39
5.1. خارطة طريق للاستفادة من تحليل وسائل التواصل الاجتماعي لحملات عمليات معلومات وزارة الدفاع الأمريكية (DoD IO) 70

الملخّص

إنّ نموّ وسائل التواصل الاجتماعي باعتبارها مصدراً فعّالاً للبيانات من أجل فهم بيئة المعلومات قد جعل منها أكثر أهميّة من أي وقتٍ مضى بالنسبة للجيش الأمريكي لتطوير قدرةٍ صلبةٍ على إجراء تحليلات بيانات وسائل التواصل الاجتماعي دعماً لعمليات المعلومات (Information Operations [IO]). وبالنظر إلى الطبيعة المُلِحّة والتحدّيات التي يقترن بها تطوير مثل هذه القدرة على حدّ سواء، وفي ضوء تقييم تم التفويض به من قِبَل الكونغرس، تحتاج وزارة الدفاع الأمريكية (U.S. Department of Defense [DoD]) بوضوح إلى إجراء دراسةٍ استقصائيةٍ بحثيةٍ للدراسات السابقة القائمة حول تكنولوجيات تحليل وسائل التواصل الاجتماعي، والممارسات الفضلى، والقيود القانونية والأخلاقية المفروضة على تحليل وسائل التواصل الاجتماعي، وتقاطع عمليات المعلومات مع تحليلات بيانات وسائل التواصل الاجتماعي.

على الرغم من ذلك، إنّها مهمّة صعبة. لم تتوقّع أُطُر العمل الحالية القانونية والخاصة بالسياسات الوتيرة السريعة والمُتناوَل العالمي لشبكات التواصل الحديثة، بما فيها وسائل التواصل الاجتماعي. تظهر أيضاً مسائل تقنية بشأن تطوير قدرةٍ صلبةٍ على تحليل وسائل التواصل الاجتماعي والتطبيقات الأكثر فائدةً لهذه التحليلات. يستكشف هذا التقرير هذه القضايا المُعقَّدة ويقدّم لوزارة الدفاع الأمريكية مجموعة من التوصيات لبناء قدرةٍ على تحليل وسائل التواصل الاجتماعي دعماً لعمليات المعلومات التي تعزّز بمهارةٍ وبشكلٍ ملائمٍ الأمن القومي.

كيف يمكن لوسائل التواصل الاجتماعي أن تدعم عمليات المعلومات

تُعرِّف وزارة الدفاع الأمريكية (DoD) **عمليات المعلومات** *(IO)* على أنّها "التوظيف المتكامل، خلال العمليات العسكرية، للقدرات المرتبطة بالمعلومات (information-related

capabilities [IRCs]) بالتضافر مع خطوط عمليات أخرى من أجل التأثير على صنع القرارات من قِبَل الخصوم والخصوم المحتملين أو تعطيله أو إفساده أو الاستيلاء عليه، مع حماية عمليّة صنع القرارات الخاصة بنا في الوقت عينه" (منشور مشترك (Joint Publication [JP] 3–13، 2014). يمكن أن تشكّل عمليات المعلومات مكوِّناً لأي نوعٍ من العمليات العسكرية، وينطوي تخطيط عمليات المعلومات على تنسيق القدرات المرتبطةً بالمعلومات — على سبيل المثال، جمع المعلومات الاستخباراتية وتحليلها، عمليات دعم المعلومات العسكرية (military information support operations [MISO])، الشؤون العامّة، أو العمليات المدنية–العسكرية — مع قدرات أخرى تولّد آثاراً في بيئة المعلومات ومن خلالها.

يقترن تحليل وسائل التواصل الاجتماعي بقدرةٍ كامنةٍ كبيرةٍ على دعم هذه العمليات من خلال توفير فهمٍ لمناظير مجموعة كبيرة من الجماهير ذات الصلة وأفكارها وأنماط تواصلها. يمكن أن توفّر هذه المنصّات معلومات مهمّة حول ديموغرافيات مجموعة أو جمهور وحجمهما وهيكليتهما التنظيمية ومجالات نشاطاتهما ومُتناوَل شبكتهما. ويمكن أن تُثير هذه التفاصيل الجهود الرامية إلى توجيه رسائل إلى جماهير معيّنة أو التأثير على تصوّراتها أو قراراتها أو سلوكها. في سياق عمليات المعلومات، على سبيل المثال، يمكن أن يحدّد تحليل وسائل التواصل الاجتماعي أفراد يتحوّلون إلى الراديكاليّة، وأن يقيس انتشار الدعم لقضايا متطرّفة ضمن ديموغرافيات محددة وأن يقيس عمق هذا الدعم.

على الرغم من أنّ تحليل وسائل التواصل الاجتماعي يقترن على الأرجح بقيمةٍ هائلةٍ بالنسبة لوزارة الدفاع الأمريكية وتُعْتَبَر وسائل التواصل الاجتماعي بدون شكّ مصدر بيانات مهمّ لعمليات المعلومات، ثمّة بعض المحدوديّات بالنسبة للاستفادة من منصّات التواصل الاجتماعي والأدوات التحليليّة. من المهمّ التذكّر أنّ بيانات وسائل التواصل الاجتماعي لا تمثّل مجموعة سكّانية بأكملها. يختلف معدّل تغلغل وسائل التواصل الاجتماعي من حول العالم، وينعكس ذلك في مجموعة البيانات المتوفرة. بالإضافة إلى ذلك، تنحرف البيانات المُتبادَلة على منصات وسائل التواصل الاجتماعي بطبيعتها نحو الذين يشاركون. وتواجه وزارة الدفاع الأمريكية أيضاً قيوداً قانونيةً مفروضةً على جمع البيانات حول الأشخاص الأمريكيين، ولذلك يعتبر من الأساسي تنفيذ إجراءات احتياطيّة من أجل تجنّب الوصول غير المصرّح به. وأخيراً، ثمّة مناطق رماديّة على مستوى السلطات التشغيلية الخاصّة بوزارة الدفاع الأمريكية بموجب القانون الفيدرالي. سيتطلّب تطوير قدرة صلبة على تحليل وسائل التواصل الاجتماعي في المقام الأول إعادة النظر في سياسات عمليات المعلومات وعملياتها.

من أجل دعم تقييم وزارة الدفاع الأمريكية للمنافع والمفاضلات وتحديّات التنفيذ التي ستواجهها وهي توسّع قدرتها على تحليل وسائل التواصل الاجتماعي، يُولِّف هذا التقرير

نتائج البحث المُستَخلَصة من مراجعةٍ للدراسات السابقة المتوفرة، مُضيفاً إليها مقابلات مع خبراء متخصصين في الموضوع داخل مؤسسة عمليات المعلومات التابعة لوزارة الدفاع الأمريكية ومجموعات التحليل الوظيفي والتجاري لوسائل التواصل الاجتماعي. باستخدام هذه المدخلات وتطبيقها على حاجات نشاطات عمليات معلومات وزارة الدفاع الأمريكية وتحدياتها الفريدة، طوّرنا مجموعة من التوصيات تهدف إلى مساعدة وزارة الدفاع الأمريكية في التنقّل في هذا المجال، مع بناء قدرةٍ تحليليةٍ صلبةٍ وفعّالةٍ خاصّة بوسائل التواصل الاجتماعي من أجل دعم العمليات من حول العالم.

التوصيات

تغطي التوصيات التالية تطوير سياسات ولغة خاصّة بوزارة الدفاع الأمريكية (DoD) لتحليل وسائل التواصل الاجتماعي، وقضايا التنفيذ العقائديّة والمؤسساتية، والاعتبارات التكنولوجية من أجل تحليل نشاط وسائل التواصل الاجتماعي بشكلٍ مفيدٍ وحشد القدرة التكنولوجيّة على إجراء تحليلات بيانات وسائل التواصل الاجتماعي على حدٍّ سواء.

التوصيات القانونية

تتمثّل خطوة أولى ضروريّة في استيفاء المتطلّبات القانونية الأمريكية بخصوص جمع بيانات وسائل التواصل الاجتماعي وتحليلها — مع تلبية حاجات الأمن القومي بفعالية — في تبيان الفَرْق الهادف بين عمليات المعلومات (IO) العسكرية بموجب الباب 10 من قانون الولايات المتحدة ومراقبة الاستخبارات الأجنبية التي يتم إجراؤها بموجب الباب 50، من الأمر التنفيذي رقم 12333 وقانون مراقبة الاستخبارات الأجنبية (Foreign Intelligence Surveillance Act). ويجب أن يشمل هذا التبيان ما يلي:

- توضيح صلة سلطة القيادة بالعمليات ونيّتها منها، بدلاً من أساليب البيانات أو مصدرها، من خلال التمييز بين العمليات المنصوص عليها في الباب 10 وتلك المنصوص عليها في الباب 50.
- التمييز بين "استخدام القوّة" في العمليات التقليدية واستخدام القدرات المرتبطة بالمعلومات (IRCs) غير الحركيّة، مثل عمليات دعم المعلومات العسكرية (MISO) أو الشؤون العامة.
- معالجة تعقيد الطبقات المتداخلة من القانون والسياسات الداخلية التي قد تنطبق على عمليات المعلومات (IO) والقدرات المرتبطة بالمعلومات (IRCs)، بالإضافة إلى أوجه الاختلاف بين القوانين الواجبة التطبيق في الولايات المتّحدة وفي دول أخرى.

- إنارة السياسات والعقيدة بمبادئ واضحة تهدف إلى حماية الأشخاص الأمريكيين بشكلٍ معقولٍ من جمع البيانات، والتمييز بين العمليات الموجّهة نحو الأشخاص الأمريكيين والعمليات التي قد تجمع بشكلٍ عرضيٍّ بيانات حول أشخاص أمريكيين كمنتجٍ ثانويٍّ للمُتَناول العالمي لأنظمة التواصل الحديثة ووسائل التواصل الاجتماعي.

تطوير اللغة الخاصة بالباب 10 لتحليل وسائل التواصل الاجتماعي

كانت وزارة الدفاع الأمريكية (DoD) تستخدم اللغة وإطار العمل المفاهيمي الخاصّين بالكيانات المنصوص عليها في الباب 50 في حين تعمل بموجب الصلاحيات المنصوص عليها في الباب 10. يجب أن تكون المصطلحات والمفاهيم متسقة عبر السياسات ونشاطات عمليات المعلومات (IO):

- بدلاً من اللغة وإطار العمل المفاهيمي (المُشار إليهما بشكلٍ ضمني) الخاصّين بالكيانات المنصوص عليها في الباب 50، يتوجّب على وزارة الدفاع الأمريكية (DoD) وضع مصطلحات متخصصة دقيقة ومميّزة للاستحواذ على بيانات وسائل التواصل الاجتماعي وتخزينها وتحليلها ويتوجب عليها دمج هذه اللغة في مذكرات العقيدة والسياسات.

التوصيات الأخلاقيّة

بالإضافة إلى ضمان الامتثال القانوني في عمليات المعلومات (IO)، يجب أن تأخذ قدرةٌ معقولةٌ ومستدامة على تحليل وسائل التواصل الاجتماعي تلبّي حاجات الأمن القومي بعين الاعتبار أيضاً المعايير الأخلاقية في الثقافة الأمريكية. تشمل توصياتنا للاعتبارات الأخلاقيّة خيارات العمليات، والممارسات الفضلى المُقترحة، وتوصيات خاصّة بشأن ضوابط الخصوصيّة:

- صياغة **مبادئ سلوك** مرنة ونشرها، بدلاً من قواعد ثابتة وراسخة، والتي تستوعب الطبيعة السريعة التطوّر لتكنولوجيات وسائل التواصل الاجتماعي واتجاهاتها.
- حيث أمكن، الإعلان عن أهداف البحث وأساليبه وجعلها واضحةً مع حماية تقنيات التجسس وإجراءاته والعمليات الجارية.
- تأسيس مبدأ "تناسب" مطوّر بشكلٍ جيّد وواضح، يحقّق التوازن بين التدخّل الناتج عن جمع البيانات وحاجات الأمن القومي المعقولة.
- اتّخاذ إجراءات احتياطيّة معقولة من أجل ضمان أنّ أساليب تخزين مجموعات بيانات وسائل التواصل الاجتماعي وتوزيعها — حتّى تلك المجهولة المصدر — تحمي الأشخاص من تحديد هويتهم من خلال الإحالة المرجعية أو الرصد التثليثي.

- تطوير ونشر معايير لقياس الخطر الذي تطرحه جهود الجمع بالنسبة للاستخدام الحرّ والمفتوح لوسائل التواصل الاجتماعي والإنترنت مقابل منافع الأمن القومي.
- تطوير ونشر معيار بشأن التوقّع المعقول للخصوصية فيما يتعلق بجمع وزارة الدفاع الأمريكية (DoD) لبيانات وسائل التواصل الاجتماعي، والذي يحقق التوازن بين حاجات الأمن القومي وتوقّعات العامّة بشأن الشفافية.

التوصيات للتنفيذ والدمج

يعالج هذا التقرير **كيفية** التمكّن من دمج تحليلات بيانات وسائل التواصل الاجتماعي بفعالية في عمليات معلومات وزارة الدفاع الأمريكية (DoD IO)، بالإضافة إلى **طرق** تنفيذ هذه المقاربات، وبالتالي، نقدّم التوصيات التالية بخصوص تنفيذ وزارة الدفاع الأمريكية لتحليلات بيانات وسائل التواصل الاجتماعي:

- استخدام القدرات المرتبطة بالمعلومات (IRCs)، بحسب ما يتمّ تعريفها في المنشور المشترك 3-13 (JP 3-13)، **عمليات المعلومات** *(Information Operations)* (2014)، باعتبارها إطار عمل لتنفيذ المقاربات التحليلية الخاصة بوسائل التواصل الاجتماعي.
- إجراء تحليل لتحديد المنافع المحتملة لجهد وزارة الدفاع الأمريكية (DoD) على مستوى المؤسسة من أجل تطوير القدرة على إجراء تحليلات بيانات وسائل التواصل الاجتماعي وإمكانياتها. قد يؤدي مثل هذا الجهد إلى وفوراتٍ كبيرةٍ في التكاليف من حيث جمع البيانات وتحليلها، والاستحواذ على التكنولوجيا، والتدريب.

التوصيات التقنيّة

تُحبّذ مراجعتنا للمقاربات التحليليّة التكنولوجيات والأساليب القائمة المفتوحة المصدر. من أجل المضي قُدُماً، يتوجب على وزارة الدفاع الأمريكية (DoD) أن تقارن تكاليف ومنافع استخدام الحلول المفتوحة المصادر مقابل الحلول التجارية. ليست التكنولوجيات أو الحلول جميعها قابلة للترجمة إلى سياقات وزارة الدفاع الأمريكية الوظيفية ووقائعها. وعلى وجه الخصوص، يتوجب على وزارة الدفاع أن تأخذ ما يلي بعين الاعتبار:

- قياس منافع مختلف الأدوات وتدفقات الأعمال وتكاليفها. قد تعمل استراتيجيات التسييل الخاصة بالكيانات التجاريّة ضدّ مصلحة الحكومة.
- طلب إمكاينة الوصول إلى العمليات الكامنة لجمع البيانات وتحليلها. يميل البائعون التجاريون إلى حجب معلومات العمليات التي تُعْتَبَر أساسية من أجل ضمان صحّة تحليلات البيانات دعماً لعمليات المعلومات (IO).

التدريب واكتساب المهارات

إنّ التدريب الحالي في مجال الاختصاصات الإلكترونية داخل وزارة الدفاع الأمريكية (DoD) غير كافٍ لدعم قدرةٍ صلبةٍ على تحليل وسائل التواصل الاجتماعي. من أجل معالجة هذا النقص، نقدّم التوصيات التالية:

- بالنظر إلى دعوات الكونغرس لوضع سياسات محددة حول استخدام وسائل التواصل الاجتماعي وغيرها من المعلومات المُتاحة للعامّة، ستدعو الحاجة إلى تدريبٍ رسميٍّ داخل وزارة الدفاع الأمريكية (DoD) حول المراقبة والامتثال.
- إلى الحدّ الذي تختار فيه وزارة الدفاع الأمريكية (DoD) بناء قدرتها على تحليل وسائل التواصل الاجتماعي باستخدام الكادر العسكري، يجب أن يتجاوز التدريب "عِلم الأزرار" لتعليم المحلّلين كيفية فهم بيانات وسائل التواصل الاجتماعي.

يقدّم الجدول S.1 خارطة طريق لوزارة الدفاع الأمريكيّة (DoD) وهي تُواصِل استكشاف العوامل المعنية بتطوير قدرةٍ على تحليل وسائل التواصل الاجتماعي وتنفيذها وتعالج التحدّيات القانونية وتلك المرتبطة بالسياسات لدى القيام بذلك.

الجدول S.1
خارطة طريق للاستفادة من تحليل وسائل التواصل الاجتماعي لحملات عمليات معلومات وزارة الدفاع الأمريكية (DoD IO)

التدبير	النتيجة
إجراء مراجعة قانونية على مستوى وزارة الدفاع الأمريكية (DoD) لدعم عمليات المعلومات (IO) من قِبَل المنظّمات المنصوص عليها في الباب 10.	إجراء تحديث على المنشور المشترك 3-13 (JP 3-13)، عمليات المعلومات (IO)، يقدّم الإرشاد القانوني والمحدوديات للقادة ومخططي عمليات المعلومات، بما في ذلك اللغة الخاصة بالباب 10 لاستخدام البيانات المتمحورة حول عمليات المعلومات
صياغة مبادئ توجيهية واضحة للاستحواذ على البيانات المتمحورة حول عمليات المعلومات (IO) وتخزينها واستخدامها ضمن وزارة الدفاع الأمريكية (DoD). يجب إنارة هذه المبادئ التوجيهية من قِبَل جهودٍ مماثلةٍ من القادة الأكاديميين والصناعيين.	مذكرة سياسات لوزارة الدفاع الأمريكية (DoD) تجعل المبادئ التوجيهية الخاصة بالسياسات واضحةً وتحدد المعايير لقياس المخاطر والمنافع للأمن القومي
تحليل نقاط القوة ونقاط الضعف لقدرة وزارة الدفاع الأمريكية (DoD) على تحليل وسائل التواصل الاجتماعي على مستوى المؤسسة، وفرص تطويرها وتكاليفه (بما في ذلك التدريب)، وخصائص التهديدات التي تواجهها.	قرار صريح على مستوى السياسات للاختيار بين إما جهود الخدمة المتخصصة/قيادة المقاتلين المحدّدة لإجراء الدراسات التحليلية الخاصة بوسائل التواصل الاجتماعي أو جهد على مستوى المؤسسة عبر وزارة الدفاع (DoD)
التكليف بإجراء مراجعةٍ مستقلّةٍ لتقديم المشورة للحكومة الأمريكية بشأن الاستحواذ على التكنولوجيا، مع التركيز على منافع ومفاضلات المصدر المفتوح مقابل استراتيجيات الاستحواذ التجاري.	مذكرة لسياسات وزارة الدفاع الأمريكية (DoD) تحدد المعايير للاستحواذ على التكنولوجيا التجارية دعماً لتحليل وسائل التواصل الاجتماعي

الاختصارات

API	application programming interface واجهة برمجة التطبيقات
AQAP	al Qaeda in the Arabian Peninsula تنظيم القاعدة في شبه الجزيرة العربية
DNN	deep neural networks الشبكات العصبية العميقة
DoD	U.S. Department of Defense وزارة الدفاع الأمريكية
IDF	Israel Defense Forces قوات الدفاع الإسرائيلي
ISIL	Islamic State of Iraq and the Levant الدولة الإسلامية في العراق والشام
IO	information operations عمليات المعلومات
IRC	information-related capability القدرة المرتبطة بالمعلومات
JP	joint publication المنشور المشترك
MILDEC	military deception التضليل العسكري
MISO	military information support operations عمليات دعم المعلومات العسكرية
NSA	National Security Agency وكالة الأمن القومي
OPSEC	operations security أمن العمليات
SNA	social network analysis تحليل الشبكات الاجتماعية

الحاجة إلى رصد وسائل التواصل الاجتماعي دعماً لعمليات معلومات وزارة الدفاع الأمريكية

تواجه وزارة الدفاع الأمريكية (DoD) والأقسام والمكوّنات والقيادات التابعة للجيش الأمريكي تحدّياً صعباً في بناء وتشغيل قدرةٍ على تحليل وسائل التواصل الاجتماعي والتي يمكن أن تدعم عمليات المعلومات (IO) والجهود الأخرى للإبلاغ أو التأثير أو الإقناع.

تُعرِّف وزارة الدفاع الأمريكية **عمليات المعلومات** على أنّها "التوظيف المتكامل، خلال العمليات العسكرية، للقدرات المرتبطة بالمعلومات (information-related capabilities [IRCs]) بالتضافر مع خطوط العمليات الأخرى من أجل التأثير على صنع القرارات من قِبَل الخصوم والخصوم المحتملين أو تعطيله أو إفساده أو الاستيلاء عليه، مع حماية عمليّة صنع القرارات الخاصة بنا في الوقت عينه" (منشور مشترك (Joint Publication 3-13, 2014 [P]). يمكن أن تشكّل عمليات المعلومات مكوّناً لأي نوعٍ من العمليات العسكرية، كما يمكن أن تشمل جهوداً تؤول إلى استخدام المعلومات باعتبارها سلعة، بالإضافة إلى نشاطات مدفوعةٍ تكنولوجياً في مجالاتٍ مثل الأمن الإلكتروني والحرب الإلكترونيّة وأمن العمليات (operations security [OPSEC]). وينطوي تخطيط عمليات المعلومات على تنسيق القدرات المرتبطة بالمعلومات — على سبيل المثال، جمع المعلومات الاستخباراتية وتحليلها، عمليات دعم المعلومات العسكرية (military information support operations [MISO])، الشؤون العامّة، أو العمليات المدنية-العسكرية — مع قدرات أخرى تولّد آثاراً في بيئة المعلومات ومن خلالها. يبحث هذا التقرير بشكلٍ محدّدٍ في كيفيّة التمكّن من تطبيق تحليل وسائل التواصل الاجتماعي بطرقٍ تدعم جهود وزارة الدفاع الأمريكية للتأثير على بيئة المعلومات.

تؤدي وسائل التواصل الاجتماعي دوراً مهمّاً ومتزايداً في عمليات المعلومات، لأن الناس من حول العالم، بما فيهم الشعوب المدنيّة، وحلفاء الولايات المتحدة، وخصوم الولايات المتحدة، يَسْتَخْدِمون منصات وسائل التواصل الاجتماعي من أجل تبادل المعلومات وإقناع الآخرين. منح النمو السريع لتكنولوجيات التواصل التي تدعم منصات وسائل التواصل الاجتماعي الخصوم غير الحكوميين منفعةً غير متماثلة:

> تميل تطوّرات الاتصالات السريعة إلى تفضيل المنظّمات الصغيرة والخفيفة الحركة والأقلّ بيروقراطية التي يمكن أن تستفيد بسرعةٍ أكبر من التقدّمات التكنولوجيّة بدون الحاجة إلى التفاوض حول عمليات الإشراف والتصاريح المطوّلة. ستنتفي منفعة وزارة الدفاع الأمريكية في الموارد الماديّة والماليّة والتكنولوجيّة في حال فشلت في تأمين موطئ قدم في فضاءات الاتصالات الناشئة هذه. ويُعتبر تحديد التقنيّات والتكنولوجيات الأكثر وعداً الخطوة الأولى الأساسية في تحديد الموقع لإثبات الصلة في بيئةٍ سريعة التغيير. (بوهنيرت [Boehnert]، 2015، ص. 13)

في حين سارع خصوم الولايات المتحدة إلى استخدام هذا الفضاء، تفتقر وزارة الدفاع الأمريكية إلى "القدرة على رصد الأدوات التحليليّة الخاصّة بوسائل التواصل الاجتماعي واستخدامها بفعالية من أجل دعم الوعي بشأن البيئة التشغيليّة لحماية القوّات والأمن التشغيلي ومهام أخرى"، بحسب تقريرٍ صادرٍ عن لجنة القوّات المسلّحة التابعة لمجلس النوّاب الأمريكي (U.S. House of Representatives Committee on Armed Services) حول قانون الإذن بمخصصات الدفاع الوطني للسنة المالية 2017 (National Defense Authorization Act for Fiscal Year 2017) (2016، ص. 246).

وبالتالي، في حين توجد أسبابٌ اضطراريةٌ مرتبطةٌ بالأمن القومي لنشر قدرةٍ على تحليل وسائل التواصل الاجتماعي، يتوجّب على وزارة الدفاع الأمريكية القيام بذلك، مع مراعاة معايير قانونية وثقافية أمريكية وفي ظلّ ظروفٍ من عدم اليقين الكبير على حدّ سواء. في وسط اتجاهات التكنولوجيات والتواصل السريعة التطوّر، يظهر خطر يتمثّل باحتمال أن تستثمر وزارة الدفاع الأمريكية في قدرات ستصبح هالكة بعد فترةٍ وجيزةٍ أو تواجه تحدّيات أخرى في بناء قدرتها التحليليّة وتطبيقها بطريقةٍ فعّالةٍ وعمليّة. بالإضافة إلى ذلك، وكما نُفصّل في الفصل التالي، يتخلّف القانون الأمريكي وسياسات وزارة الدفاع الأمريكية باستمرار عن الواقع التقني لتكنولوجيات التواصل وأنماطه السريعة التوسّع والتحوّل التي تمّ اعتمادها بهذه الطريقة السريعة والخفيفة الحركة من قِبَل الخصوم. ويتجاوز هذا التحدّي العمليات العسكرية الأمريكية حيث تتعامل الأوساط الأكاديمية والبحثية الأمريكية مع عدم يقينٍ مماثل. على الرغم من ذلك، تتمثّل النتيجة بالنسبة لوزارة الدفاع الأمريكية بأنّ وحدات الاستخبارات غالباً ما تتصرّف بدون وضوحٍ كاملٍ حول كيفيّة جمع بيانات وسائل التواصل الاجتماعي وتحليلها بشكلٍ قانونيٍّ وأخلاقيٍّ وفعّال.

تُعدّ الحاجة إلى أدوات لتحليل وسائل التواصل الاجتماعي ملحّةً جداً لدرجة أنّ الكونغرس قد أصدر توجيهاً لوزير الدفاع (Secretary of Defense) من أجل تقييم سياسات وزارة الدفاع الأمريكية حول الموضوع وتحديد ما يلي:

- الطلب في صفوف قيادات المقاتلين الأمريكيّة على مثل هذه القدرات، بالإضافة

إلى تقريرٍ حول الفجوات أو النقاط الحاليّة حيث تدعو الحاجة إلى التوضيح على صعيد السياسات، والعقيدة، والتدريب والقدرات التكنولوجيّة.

- المهام التشغيلية التي تدعو الحاجة فيها إلى تحليل وسائل التواصل الاجتماعي، مع أمثلة تشمل الوعي حول فضاء المعركة، وأمن العمليات (OPSEC)، والرسائل المضادة، والاستخدام التشغيلي للمعلومات المُتاحة للعامّة[1]
- القضايا القانونية وتلك على مستوى السياسات والمرتبطة باستخدام المعلومات المُتاحة للعامّة
- المحدوديّات على مستوى الموارد، وعمليات الموافقة، ومتطلّبات التدريب التي تؤثّر على استخدام وزارة الدفاع الأمريكية (DoD) للمعلومات المُتاحة للعامّة، بالإضافة إلى الخطوات التي تتخذها الوزارة من أجل تحسين التنسيق والاستفادة من الممارسات والقدرات الفضلى
- خطط وزارة الدفاع الأمريكية (DoD) من أجل ضمان أنّ العمليّات لا تنتهك خصوصية الأشخاص الأمريكيين وأن الإجراءات الاحتياطيّة قائمة من أجل منع الوصول غير المصرّح به إلى المعلومات (مجلس النوّاب الأمريكي [U.S. House of Representatives]، لجنة القوّات المسلّحة [Committee on Armed Forces]، 2016، ص. 241).

غرض هذا التقرير ونطاقه

بالنظر إلى الطبيعة المُلِحّة والتحدّيات التي يقترن بها تطوير قدرة على تحليل وسائل التواصل الاجتماعي، وفي ضوء تقييم تم التفويض به من قِبَل الكونغرس، طلب مكتب الدعم التقني لمكافحة الإرهاب التابع لوزارة الدفاع الأمريكية (DoD's Counterterrorism Technical Support Office) إجراء دراسةٍ استقصائيةٍ بحثيةٍ

[1] يعرّف كتيّب وزارة الدفاع الأمريكية 01.5240، "الإجراءات التي ترعى الاضطلاع بنشاطات استخبارات وزارة الدفاع الأمريكية" (*DoD Manual 5240.01, Procedures Governing the Conduct of DoD Intelligence Activities*) الذي تم نشره مؤخراً، المعلومات المُتاحة للعامّة كالتالي:

> المعلومات التي يتمّ نشرها أو بثّها للاستهلاك العامّ، أو تكون مُتاحة للعامّة بناءً على الطلب، أو يمكن الوصول إليها من قِبَل العامّة على الإنترنت أو بخلاف ذلك، أو تكون مُتاحة للعامّة من خلال الاشتراك أو الشراء، أو يمكن رؤيتها أو سماعها من قِبَل أي مراقِب عاديّ، أو يتمّ توفيرها خلال اجتماعٍ مفتوحٍ للعامّة، أو يتم الحصول عليها من خلال زيارة أي مكان أو حضور أي حدث مفتوحين للعامّة. وتشمل المعلومات المُتاحة للعامة المعلومات التي تكون مُتاحة بشكلٍ عامّ للأشخاص في المجموعة العسكرية على الرغم من أنّ المجموعة العسكرية ليست مفتوحةً لعامّة الجمهور المدني. (كتيّب وزارة الدفاع الأمريكية 01.5240 [DoD Manual 5240.01]، 2016، ص. 53)

للدراسات السابقة القائمة حول تكنولوجيات تحليل وسائل التواصل الاجتماعي، والممارسات الفضلى، والقيود القانونية والأخلاقية المفروضة على تحليل وسائل التواصل الاجتماعي، وتقاطع عمليات المعلومات (IO) مع تحليل وسائل التواصل الاجتماعي. يُؤلِّف هذا التقرير النتائج المستخلصة من البحث بهدف رسم خريطة لـ"أرضيّة" القضايا التي ستواجهها وزارة الدفاع الأمريكية في المستقبل القريب وهي تُطَوّر خطط لتشغيل تكنولوجيات وتقنيّات جديدة لتحليل وسائل التواصل الاجتماعي وتوفير سياقٍ لمناقشةٍ مستنيرةٍ حول هذه الخطط ونتائجها. بالاعتماد على مراجعةٍ للدراسات السابقة المتوفرة، بالإضافة إلى مقابلات مع خبراء متخصصين في الموضوع، نقدّم مجموعة من التوصيات المصمّمة من أجل مساعدة وزارة الدفاع الأمريكية في التنقّل في هذا المجال، مع بناء قدرةٍ تحليليةٍ صلبةٍ وفعالّةٍ خاصّة بوسائل التواصل الاجتماعي من أجل دعم العمليات من حول العالم.

من أجل تعزيز فائدة نتائج هذه الدراسة وطول مدّتها، تعالج الفصول الأساسيّة لهذا التقرير تحليل وسائل التواصل الاجتماعي بطريقةٍ عامّةٍ وترتكز إلى المقاربة. حتّى مع تغيّر تكنولوجيات وسائل التواصل الاجتماعي ومنصّاتها، يجب أن تبقى المفاهيم والممارسات ذات صلة بمهمّة وزارة الدفاع الأمريكية.

يعالج هذا التقرير بالتحديد استخدام الجيش الأمريكي لتحليل وسائل التواصل الاجتماعي دعماً لعمليات المعلومات، مثل استخدام بيانات وسائل التواصل الاجتماعي لفهم المواقف والمخاوف المحلّية في منطقةٍ معيّنةٍ بشكلٍ أفضل. لا يشمل استخدام وسائل التواصل الاجتماعي باعتباره منصّة بثّ يتم تنفيذ عمليات المعلومات انطلاقاً منها — على سبيل المثال، من خلال استخدام المدوّنات الصغرى لمحاولة إقناع الشعوب المحليّة لدعم العمليات العسكرية الأمريكية.

لا شكّ في أنّ وسائل التواصل الاجتماعي هي مجرّد مجموعة فرعية من عالمٍ أكبر بكثير من المعلومات المُتاحة للعامّة (راجع كتيّب وزارة الدفاع الأمريكية 01.5240 [DoD Manual 5240.01]، 2016). إنّ سياسات وزارة الدفاع الأمريكيّة وقدرة الوزارة على تحليل وسائل التواصل الاجتماعي مُقيّدة ضمن القضية الأكبر بشأن كيفية التعامل مع المعلومات المُتاحة للعامّة، وإنّنا نقرّ بقيمة هذه المعلومات. فعلى سبيل المثال، قد تساعد أنماط استخدام جهاز الهاتف الجوّال أو تفضيلات المُستَخدِمين لنوعٍ معيّن من الأجهزة والمُبلَّغ عنها ذاتياً المحلّلين على فهم بيئة المعلومات في منطقة معيّنة بشكلٍ أفضل. وتشكّل كيفية استخدام المعلومات المُتاحة للعامة بالطريقة الفضلى موضوع يستحقّ المزيد من الدراسة. وعلى الرغم من ذلك، ينظر هذا التقرير بالتحديد في تحليل وسائل التواصل الاجتماعي، وليس المعلومات المُتاحة للعامّة واستخدامها بشكلٍ واضح.

مقاربة الدراسة وأساليبها

يُولِّف هذا التقرير النتائج المُستخلصة من البحث ذي الصلة حول المفاهيم والتطبيقات والتحديّات التحليلية الخاصة بوسائل التواصل الاجتماعي، بالإضافة إلى الدراسات السابقة حول عمليات المعلومات (IO) بشكلٍ واضح. تشكّلت مصادر الدراسات السابقة في المقام الأوّل من الأبحاث الأكاديمية والتي جرت برعاية وزارة الدفاع الأمريكيّة (DoD)، وإنّما شملت أيضاً مجلّات قانونية، وتقارير صناعيّة وبعض المصادر الصحفية. اعتمدنا كذلك على الدراسات السابقة من أوساط البحث الأكاديمية التي تحاول بحد ذاتها التعامل مع الممارسات والقواعد التي لا تأخذ وسائل التواصل الاجتماعي بعين الاعتبار بوصفها موقعاً جديداً للبحث. تعرض الفصول المتتالية أمثلة من هذه الدراسات ذات الصلة بعمليات المعلومات.

استكملنا بحثنا بإجراء خمس مقابلات مع خبراء متخصصين في الموضوع داخل مؤسسة عمليات المعلومات التابعة لوزارة الدفاع الأمريكية (DoD IO) ومجموعات تحليل وسائل التواصل الاجتماعي الوظيفية والتجارية. كان غرضنا تحديد الممارسات والأساليب التحليليّة والمخاوف التي تُعتبر ذات صلة حالياً أو بشكلٍ محتملٍ بمهمّة عمليات معلومات وزارة الدفاع الأمريكية. لا تمثّل مقابلاتنا عيّنة قابلة للتعميم من مناظير الخبراء، وإنّما تقدّم بالفعل منظوراً يقوم على أساس تشغيلي من أفراد عمليات المعلومات النظاميين والمدنيين من مختلف أقسام وزارة الدفاع الأمريكية والذين يتمتعون بخبرة كبيرة في المقاربات والتحدّيات التي تتم معالجتها في هذا التقرير. كانت المقابلات سرّيّة من أجل تشجيع هؤلاء الخبراء على التكلّم بحرّيّة والاعتماد على مناظيرهم وتجربتهم الشخصيّة. ولأنّ هذه المقابلات كانت مُصمّمة من أجل الحصول على معلومات تقنيّة محدّدة، وليس معرفة قابلة للتعميم، وجد مجلس المراجعة المؤسساتية التابع لمؤسسة RAND (RAND's Institutional Review Board) أنّ مشروعنا لا يتطلب حماية المشاركين في البحث.

هيكلية هذا التقرير

يستكشف ما تبقّى من هذا التقرير كيف يمكن لوزارة الدفاع الأمريكية (DoD) أن تبدأ بالتفكير في تنفيذ تحليل وسائل التواصل الاجتماعي دعماً لعمليات المعلومات (IO). ويتمّ استكمال المناقشة بعددٍ من الأمثلة حول كيفية التمكّن من استخدام هذه المقاربات في سياقات محددة من عمليات المعلومات، والمحدوديات المفروضة على استخدام هذه البيانات، وأطر العمل القانونية وتلك الخاصة بالسياسات والتي يتوجّب على وزارة الدفاع الأمريكية العمل في ظلّها.

يجادل الفصل الثاني أنّ تحليل وسائل التواصل الاجتماعي أساسيّ لتنفيذ عمليات المعلومات بفعالية حالياً وفي المستقبل. ولأنّ تحليل وسائل التواصل الاجتماعي هو مفهوم جديد نسبياً، نرسم إطاراً للمناقشة من حيث القدرات المرتبطة بالمعلومات (IRCs) والتي تُعْتَبر مجموعة عمليات المعلومات على اطّلاع عليها أصلاً. يقدّم الفصل بعدئذٍ إطار عمل للتفكير في المقاربات التحليلية الخاصة بوسائل التواصل الاجتماعي وتطبيقها، بالإضافة إلى أمثلة عن التطبيقات لمختلف القدرات المرتبطة بالمعلومات.

يقدّم الفصل الثالث لمحة عامّة حول الممارسات والمقاربات التحليليّة الفضلى الحاليّة، ولكنّ المناقشة لا تقتصر على التكنولوجيا الحاليّة. بالاعتماد على خبرة مؤسسة RAND ودورها الريادي في تحليل وسائل التواصل الاجتماعي وتحليلات بياناتها، يركّز الفصل على فائدة البيانات النصيّة والصورية بالنسبة لعمليات المعلومات والأساليب التي يمكن أن ترفع هذه الفائدة إلى أقصى حدّ. ونقدّم أيضاً نموذجاً مفاهيمياً للتفكير في مستويات تحليل بيانات وسائل التواصل الاجتماعي وكيف يمكن أن ينير كل مستوى من التحليل عمليات المعلومات.

ينظر الفصل الرابع في أطر العمل القانونية والأخلاقية الأمريكية لتحليل وسائل التواصل الاجتماعي والتحدّيات بالنسبة لعمليات المعلومات، على وجه الخصوص، مقدّماً سياقاً لأسئلة غير تقنيّة حول استخدام وسائل التواصل الاجتماعي باعتبارها جزءاً من عمليات المعلومات.

يختتم الفصل الخامس هذا التقرير مع سلسلةٍ من التوصيات الخاصّة بتنفيذ تحليل وسائل التواصل الاجتماعي بطريقةٍ تدعم مهمة وزارة الدفاع الأمريكية وتفي بمتطلبات الإشراف. إن التوصيات صادرة عن جهات مزوّدة محايدة من حيث الدعم والاستحواذ لضمان إمكانية تطبيقها على مجموعة من النشاطات والمبادرات. ويشمل الفصل أيضاً توصيات مرتبطة بالمتطلبات القانونية والأخلاقية الأمريكية، وبناء القدرة على تحليل وسائل التواصل الاجتماعي لدعم عمليات المعلومات وتعميم المنتجات التحليلية الخاصة بوسائل التواصل الاجتماعي.

كيف يمكن لتحليل وسائل التواصل الاجتماعي أن يدعم عمليات المعلومات

يقترن تحليل وسائل التواصل الاجتماعي بقدرةٍ كامنةٍ كبيرةٍ على دعم عمليات معلومات وزارة الدفاع الأمريكيّة (DoD) لأنّه يوفّر فهماً لمناظير مجموعةٍ كبيرةٍ من الجماهير ذات الصلة وأفكارها وأنماط تواصلها. تساهم المنظّمات والمُستَخدِمون الفرديون على حدّ سواء في مجموعات بيانات وسائل التواصل الاجتماعي الغنيّة بشكلٍ محتملٍ من خلال منشوراتهم العامّة. فعلى سبيل المثال، يمكن أن توفّر منصّات وسائل التواصل الاجتماعي معلومات مهمّة حول ديموغرافيات مجموعة أو جمهور وحجمهما وهيكليتهما التنظيمية ومجالات نشاطاتهما ومُتَناول شبكتهما. ويمكن أن تُثير هذه التفاصيل الجهود الرامية إلى توجيه رسائل إلى جماهير معيّنة أو التأثير على تصوّرات مجموعةٍ أو قراراتها أو سلوكها. تُعتبر هذه المعلومات ذات صلة بالتحديد بعمليات المعلومات (IO) عندما تتعلّق بمجموعات تكون أساسيّة بالنسبة لنتيجة العمليات العسكريّة، بغضّ النظر عمّا إذا كانت المجموعة خصماً، أو مجموعة داعمة من أي طرف من الصراع، أو ضروريةً لدعم الوضع النهائي المرجو لحملة معلومات.

على سبيل المثال، يمكن استخدام التحليل النصّي من أجل تحديد أفراد يتحوّلون إلى الراديكاليّة، وقياس انتشار الدعم لقضايا متطرّفة ضمن ديموغرافيات محددة وقياس عمق هذا الدعم (كوريا وسوريكا [Correa and Sureka]، 2013). يمكن أن تستكمل المنشورات التي تحمل الوسم الجغرافي تحليل وسائل التواصل الاجتماعي، مُساعِدةً ممارسي عمليات المعلومات في تحديد الانتشار الجغرافي للأفكار أو مجالات الدعم القويّ أو الضعيف بشكلٍ خاص لقضية أو مجموعة أو فكرة. يوفّر تحليل الشبكات منافع محتملة إضافيّة في التخطيط للجهود الرامية إلى تعزيز انتشار أفكار أو معلومات محدّدة أو مكافحتها. يمكن أن يساعد تحليل البيانات التي تولّدها المنشورات على وسائل التواصل الاجتماعي مقابل البيانات الوصفيّة والديموغرافيّات الخاصّة بالمُستَخدِمين المُرتبطين بالحسابات في تحديد المؤثّرين في شبكةٍ اجتماعيّة، مُتيحاً لحملات المعلومات استهداف المجموعات أو الأفراد الأكثر قابليّة للتأثير. يمكن أن تجمع خوارزميّات تصنيف

الصور وتَصِف أنواع الصور التي يتم تبادلها على وسائل التواصل الاجتماعي، والتي، لدى تحليلها إلى جانب بيانات أخرى مع برمجيات الاستدلال الجغرافيّ ورسم الخرائط، قد تسمح لممارسي عمليات المعلومات بتجسيد التغيّرات على مستوى تفضيلات الشعوب المحلية ومواقفها تجسيداً مرئياً.

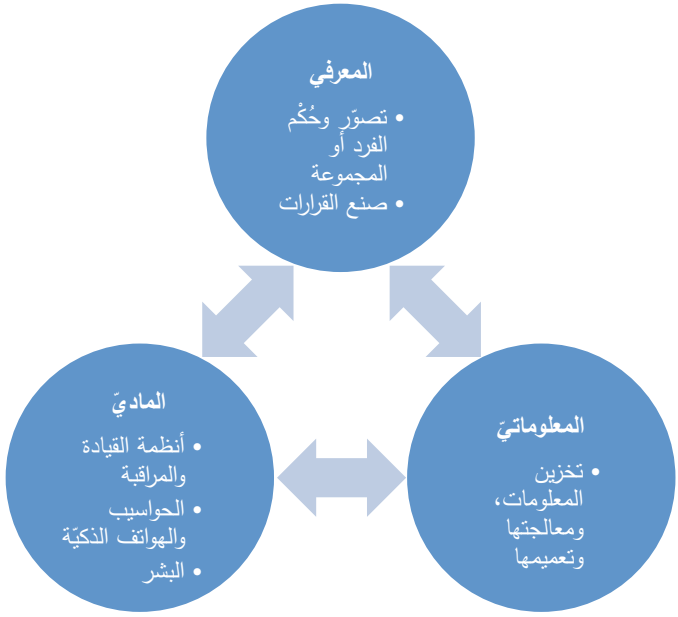
في هذا الفصل، ننظر في قدرة وسائل التواصل الاجتماعي الكامنة على إنارة عمليات المعلومات ودعمها. نستخدم القدرات المرتبطة بالمعلومات (IRCs) بوصفها إطار عمل قائم، مع الإشارة إلى كيفية التمكّن من استخدام تحليل وسائل التواصل الاجتماعي باعتباره مصدراً للبيانات ومجموعةً من الأساليب التحليلية عَبْر قدرات مرتبطة بالمعلومات متعدّدة، على حدّ سواء. تُعتبر عمليات المعلومات والقدرات المرتبطة بالمعلومات مفاهيم مألوفة بالنسبة لممارسي عمليات المعلومات وهي بالتالي تشكلّ ميزات لعقيدة وزارة الدفاع الأمريكية. بهذه الطريقة، نستخدم القدرات المرتبطة بالمعلومات باعتبارها إطار عمل من أجل ربط الأساليب والتكنولوجيات الجديدة بممارسة وزارة الدفاع الأمريكية الحاليّة.

يمكن أن يساعد تحليل وسائل التواصل الاجتماعي ممارسي عمليات معلومات وزارة الدفاع الأمريكية (DoD IO) على فهم الجهود التي يبذلها الخصوم من أجل جمع المعلومات الاستخباراتية بشكلٍ أفضل وتحديد الشبكات ذات الأهميّة، وجمع المعلومات الاستخباراتية عن بُعْد على مستويات مُفصَّلَة إلى حدّ ما. يمكن أيضاً تطبيقه في الجهود الرامية إلى قياس الرأي العام، وقياس العمليات ذات التأثير العكسي وكشفها، والتأثير على تقنيات التجسس وإجراءاته. يمكن مراجعة حملات أمن العمليات (OPSEC) والتضليل العسكري (Military Deception [MILDEC]) على حدّ سواء في حال كَشَفَ تحليل وسائل التواصل الاجتماعي عن انتهاكات لأمن العمليات أو عن مؤشرات على أنّ التضليل قد فشل، وبالتالي حماية المعلومات الحسّاسة من الخصوم المحتملين. وأخيراً، ننظر في كيفية تمكّن تحليل وسائل التواصل الاجتماعي من دعم جهود الشؤون العامة، والمساعدة في الاستفادة من العمليات المدنية–العسكرية وتيسير انخراط القادة الرئيسيين.

بيئة المعلومات والقدرات المرتبطة بالمعلومات

عزّز الاستخدام المتزايد للتواصل الإلكتروني وتبادل المعلومات على حدّ سواء القدرة على التواصل وتبادل كميّات كبيرة من البيانات بسرعة وأدخل نقاط ضعف جديدة. تؤثّر نقاط الضعف هذه على كل واحد من الأبعاد المادّيّة والمعلوماتيّة والمعرفيّة لبيئة المعلومات المحددة في المنشور المشترك 3–13 (JP 3–13). يجسّد الشكل رقم 2.1 مرئياً هذه الأبعاد بوصفها مميزةً وإنّما مترابطة. فعلى سبيل المثال، قد يكون لخسارة القدرة المعلوماتيّة تأثيرات مهمّة على صنع القرارات في الدائرة المعرفية وعمل هندسة

الشكل رقم 2.1
مكوّنات بيئة المعلومات



المصدر: مُستخرج من المنشور المشترك 3-13 (JP 3-13)، 2014.

RAND *RR1742-2.1*

الشبكات في الدائرة المادّيّة.

القدرات المرتبطة بالمعلومات هي الأدوات والنشاطات التي يستخدمها قائد للحدّ من نقاط الضعف ولاستغلال الخصوم والتأثير عليهم في بيئة المعلومات. في هذا التقرير، نركّز على القدرات المرتبطة بالمعلومات التي تنطبق عليها بيانات وسائل التواصل الاجتماعي بالشكل الأكبر، لا سيّما الاستخبارات، والتأثير (عمليات دعم المعلومات العسكرية) (MISO)، وأمن العمليات (OPSEC)، والتضليل العسكري (MILDEC)، والشؤون العامّة، والعمليات المدنية–العسكرية، وانخراط القادة الرئيسيين. ويلخّص الجدول رقم 2.1 كيفية تعريف القدرات المرتبطة بالعمليات هذه في عقيدة وزارة الدفاع الأمريكية.

ويراجع ما تبقّى من هذا الفصل كل قدرة مرتبطة بالمعلومات ويقدّم أمثلة حول كيفية تمكّن تحليل وسائل التواصل الاجتماعي من إنارة هذه القدرات وتعزيزها.

الجدول رقم 2.1
أنواع القدرات المرتبطة بالمعلومات (IRC) وتعريفاتها

القدرة المرتبطة بالمعلومات (IRC)	التعريف
الاستخبارات	توفّر "معلومات استخباراتيّة اجتماعية ثقافية تتمحور حول الشعب وتأسيسات الشبكة المادية، بما في ذلك المعلومات التي يتم نقلها عَبْر هذه الشبكات"
عمليات دعم المعلومات العسكرية (MISO)	"العلميات المُخطط لها من أجل نقل المعلومات والمؤشرات المختارة إلى الجماهير الأجنبية من أجل التأثير على عواطفهم، ودوافعهم، وتفكيرهم الموضوعي، وفي نهاية المطاف على سلوك الحكومات الأجنبية"
أمن العمليات (OPSEC)	"عملية موحّدة مصمّمة لتلبية الحاجات التشغيلية من خلال الحدّ من المخاطر المرتبطة بنقاط ضعف محددة من أجل إنكار معلومات الخصوم الحرجة والمؤشرات التي يمكن ملاحظتها"
التضليل العسكري (MILDEC)	"الأعمال التي يتم تنفيذها من أجل تضليل صانعي القرارات الخصوم عمداً"
الشؤون العامّة	"معلومات العامّة، ومعلومات القيادة، ونشاطات إشراك العامّة الموجّهة نحو العامة الداخلية والعامة الخارجية على حدّ سواء والمهتمة بوزارة الدفاع الأمريكية (DoD)"
العمليات المدنية–العسكرية	العمليات من أجل "تأسيس علاقات بين القوات العسكرية والمنظّمات والسلطات الحكومية والمدنية غير الحكومية والسكّان المدنيين أو المحافظة عليها أو التأثير عليها أو استغلالها في منطقة تشغيلية ودية أو محايدة أو عدائية من أجل تحقيق الأغراض الأمريكية"
انخراط القادة الرئيسيين	"حالات الانخراط التي يمكن استخدامها من أجل تشكيل القادة الأجانب والتأثير عليهم على الأصعدة الاستراتيجية والتشغيلية والتكتيكية"

المصدر: المنشور المشترك 3–13 (JP 3–13)، 2014.

الاستخبارات

إن حجم المعلومات المنشورة على وسائل التواصل الاجتماعي ونطاقها يجعلان هذه المنصّات مكاناً محفوفاً بالتحديّات ومثالياً على حدّ سواء لجمع المعلومات الاستخباراتية. فعلى سبيل المثال، ينشر مُستَخدمو تويتر (Twitter) وحدهم 500 مليون تغريدة كل يوم (أوريسكوفيك [Oreskovic]، 2015). وينشر المُستَخدِمون الصور ومقاطع الفيديو وتحديثات بشأن الحالة على وسائل التواصل الاجتماعي وغالباً ما تشمل ملفاتهم الشخصيّة تفاصيل شخصية مثل عمرهم، وجنسهم، وأفراد عائلتهم ومكان عملهم. توفّر هذه المنشورات رؤية حول حياة الأفراد اليوميّة، بالإضافة إلى المواقف والسلوكيّات المرتبطة بالشبكات الاجتماعية. يُعتبر من الممارسة الشائعة الآن بالنسبة للشركات

الكبيرة استخدام تحليلات بيانات وسائل التواصل الاجتماعي من أجل فهم قاعدة زبائنها بشكلٍ أفضل، وتوجيه قرارات التسويق وتطوير المنتجات (مقابلة مع خبير متخصص في الموضوع، 1 سبتمبر/أيلول 2016). تستخدم الشركات خدمات مثل توبسي (Topsy) (التي استحوذت عليها أبل [Apple] عام 2013) وسبرينكلر (Sprinklr) من أجل تحليل بيانات وسائل التواصل الاجتماعي وإنارة الاستراتيجيات من أجل إشراك الزبائن وتوجيه جهودها التسويقية بشكلٍ أفضل. تقدّم هذه الخدمات تحليلات معمّقة للجماهير التي تشاهد منشورات الشركات ولكيفية انخراط هذه الجماهير مع الشركة ومع آخرين على الإنترنت على حد سواء. قد تُنتج القدرة على جمع البيانات من مصادر مختلفة تحليلاً قيّماً جدّاً، وقد شكّل ذلك موضوعاً متكرراً في مقابلاتنا مع الخبراء.

قدّمت السنوات المتعددة الماضية أمثلة كثيرة حول بيانات وسائل التواصل الاجتماعي باعتبارها مصدراً لمعلومات استخباراتية قيّمة بالنسبة للحكومة والكيانات التجاريّة على حد سواء. لفت منشور يحمل الوسم الجغرافي على حساب مقاتلٍ على وسائل التواصل الاجتماعي انتباه وحدة القوى الجوية التابعة للولايات المتّحدة (U.S. Air Force) التي استخدمت المعلومات من أجل إطلاق حملة قصف على مبنى تتّخذه الدولة الإسلامية في العراق والشام (Islamic State in Iraq and the Levant [ISIL]) مقرّاً لها، عام 2015 (راجع إيفرستاين [Everstine])، 2015). استخدمت شركات الشحن منشورات قراصنة صوماليين على تويتر (Twitter) وفيسبوك (Facebook) من أجل فهم كيفية استهداف المنظّمات الإجرامية للسفن والتخطيط لهجماتهم فهماً أفضل (لايه [Lahe]، 2012). ويمكن أن يعزز التعليم الآلي والأساليب الأخرى المُستَخدَمة لمعالجة الكميات الكبيرة من المعلومات المنشورة على وسائل التواصل الاجتماعي عملية الأوساط الأمنية لجمع البيانات حول التهديدات والأحداث الأمنية بشكلٍ آني، مُحسّنةً التوقعات بشأن مجالات انعدام الاستقرار المستقبلية. ويمكن أن توفّر هذه البيانات أيضاً رؤى حول نشاطات المجموعات الإجرامية أو الإرهابية وتساعد على تحديد الأعضاء وأماكن تجمّعهم.

فهم الشبكات من خلال تحليل بيانات وسائل التواصل الاجتماعي

يمكن أن تحدّد خرائط علاقات المُستَخدِمين الفرديين وتفاعلاتهم على منصّات وسائل التواصل الاجتماعي، بشكلها الأكثر أساسية، أعضاء مجموعةٍ محددة. تَمَكَّن الباحثون من الكشف عن فروقاتٍ دقيقةٍ في ديناميكيات الشبكات الشخصية بين الأفراد من خلال تحليل المعلومات التي ينشرها المُستَخدمون على هذه المنصّات. فمن خلال النظر في علاقات الأتباع على تويتر (Twitter)، تَمَكَّن الباحثون من رسم خارطةٍ لشبكات الآراء بالاعتماد على مناقشات السياسات الخارجيّة للمواجهة الإيرانيّة–الإسرائيليّة حول برنامج إيران النووي (زيتزوف [Zeitzoff]، كيلي [Kelly] ولوتان [Lotan]، 2015). عكست

شبكات الآراء هذه على الإنترنت أوجه اختلاف السياسات في العالم الحقيقي غير الافتراضي، موفّرةً أسلوباً قيّماً لتحديد أعضاء مجموعات ذات آراء مختلفة. لهذا البحث تداعيات تتجاوز شبكات الآراء البسيطة؛ يمكن استخدامه أيضاً من أجل تحديد الأفراد الذين يتحوّلون إلى الراديكاليّة أو الذين من المرجّح أن يرتكبوا جرماً.

ثمّة قيمة محدّدة في قدرة بيانات وسائل التواصل الاجتماعي على الكشف عن الاتجاهات الإقليمية. وجد الباحثون أنّه عندما حصلت زيادات كبيرة في مناقشة الإيرانيين حول حدثٍ أو قضيةٍ على وسائل التواصل الاجتماعي بدون أن تحصل زيادة مقابلة في المنشورات في بلدان أخرى، لم يتم اختيار تغطية القضية من قِبَل وسائل الإعلام الرئيسية (زيتزوف [Zeitzoff]، كيلي [Kelly] ولوتان [Lotan]، 2015). قد تكون التغيّرات الخاصّة بالبلد أو المنطقة في الرأي العام أو الانحرافات في اللغة والنبرة المُستَخدَمة لمناقشة قضية معلومات قيّمةً في بيئة صراع.

يشير تقريرٌ أخيرٌ صادر عن مؤسسة بروكينغز (Brookings Institution) إلى كيفية التمكّن من استخدام تحليل وسائل التواصل الاجتماعي والشبكات من أجل جمع المعلومات حول منظمة مُستَهدَفة. حلّل المؤلفون عيّنةً تتألّف من 20,000 حساب مُستَخدِم على تويتر تُعبّر عن الدعم للدولة الإسلامية في العراق والشام (ISIL)، مُستَخرِجين معلومات حول موقع المناصرين ومستوى نشاطهم، واللغات الأكثر استخداماً في تغريداتهم، وعدد مُستخدِمي تويتر الذين يتبعون هذه الحسابات. وجدوا أنّ جزءاً كبيراً من نجاح المجموعة يمكن أن يعزى إلى عددٍ صغيرٍ نسبياً من المُستَخدِمين الكثيري النشاط في سوريا والعراق ومناطق أخرى مُتنازع عليها من قِبَل الدولة الإسلامية في العراق والشام (برغر [Berger] ومورجان [Morgan]، 2015).

يوفّر تقرير أجرته مؤسسة RAND تحليلاً مفصّلاً أكثر بعد لشبكة الدولة الإسلامية في العراق والشام على تويتر. **داعش** *(Daesh)* هو مصطلح عربي يُستخدم بشكلٍ عامٍ في الشرق الأوسط من قِبَل الذين يُعارضون المجموعة، في حين يستخدم المناصرون تركيبات مختلفة لعبارة **الدولة الإسلامية** *(Islamic State)*. من خلال استخدام هذه المصطلحات للتمييز بين حسابات المُستَخدِمين الذين أيّدوا الدولة الإسلامية في العراق والشام عن هؤلاء الذين عارضوا هذه المجموعة، تمكّن المؤلّفون من إجراء تحليل للشبكات لكل معسكر مُعارض وتقييم كيفية تفاعل هذه المجموعات البعض منها مع البعض الآخر (بودين–بارون [Bodine–Baron]، مارسيلينو وآخرون [Marcelino et al.]، 2015). قد يكون تقييم الذين يتفاعلون مع مناصري الدولة الإسلامية في العراق والشام وكم مرّة يقومون بذلك قيّماً لزيادة فهم المجموعة وتحديد المؤثّرين الرئيسيين، أو الذين يُعتبرون الأكثر قدرةً على إبعاد المناصرين عن الدولة الإسلامية في العراق والشام. وكما هي الحال في دراسة مؤسسة بروكينغز، نتج عن تحليل مؤسسة RAND للتغريدات التي تحمل

وسماً جغرافياً رؤى حول الانتشار الجغرافي لمناصري الدولة الإسلامية في العراق والشام. بهذه الطرق، يمكن أن تَسْتَكْمِل المعلومات التي توفّرها وسائل التواصل الاجتماعي وتُنير جمع المعلومات الاستخباراتيّة وتحليلها.

التحقّق من موثوقيّة بيانات وسائل التواصل الاجتماعي ودقّتها

استُخدِمت وسائل التواصل الاجتماعي من أجل التحقّق على الفور من مصادر خارجية من التطوّرات والأحداث، مع تحسين التوعية بالأوضاع السائدة لقوات الأمن. عندما تحصل أحداثٌ رئيسيّة، من المرجّح أن ينشر المُستَخدِمون منشورات بشأنها على وسائل التواصل الاجتماعي، محوّلين حتّى المشاهدين الخاملين إلى "صحافيين مواطنين يوفّرون وينقلون المعلومات من الأرض"، وغالباً بشكلٍ آني (أوماند [Omand]، بارتليت [Bartlett]، وميلير [Miller]، 2012). فعلى سبيل المثال، خلال أعمال الشغب في لندن ومدن إنجليزية أخرى في أعقاب حادثة إطلاق النار من قِبَل الشرطة والتستّر المزعوم عام 2011، أسّست الشرطة منصّة على الإنترنت سمحت للمواطنين بنشر تحديثات حول الحالة في مجموعاتهم وتحديد الذين تورّطوا في أعمال النهب والعنف من مجموعة من الصور للمشتبه بهم نشرتها وكالات إنفاذ القانون. وجد تحليل الحركة على تويتر (Twitter) خلال هذه الفترة أنّ موجات التغريدات غالباً ما كانت تسبق تقارير الأخبار التقليدية حول حدثٍ رئيسيّ (أوماند [Omand]، بارتليت [Bartlett]، وميلير [Miller]، 2012). تمكّنت وكالات إنفاذ القانون من استخدام هذه المعلومات من أجل تحسين التوعية بالأوضاع السائدة والاستجابة للأحداث بسرعةٍ أكبر. في حين أنّ هذا الشكل من المشاركة يتجاوز الرصد البسيط، يمكن تخيُّل جهدٍ مماثلٍ حيث يحلل ممارسو عمليات المعلومات (IO) بيانات وسائل التواصل الاجتماعي حول أعمال شغب تندلع في بلدٍ حيث تعمل القوات الأمريكية، مُستخدِمين هذه البيانات للتخطيط لتدخّلات من أجل الحدّ من انتشار الفوضى، وتحديد المحرّضين، وربّما فضح أفراد محدّدين أو إهانتهم أو التأثير عليهم أو توقيفهم.

في حين تقترن بيانات وسائل التواصل الاجتماعي بتحيّز واضح من حيث أخذ العيّنات — يمكن أن يقيّم المحلّلون المعلومات التي يختار المُستخدِمون إتاحتها للعامّة فحسب، ويميل مُستخدِمو وسائل التواصل الاجتماعي إلى كونهم شباب، وحضريين ومتعلّمين تعليماً جيداً — تملك هذه البيانات القدرة الكامنة على توفير رؤى قيّمة حول الأحداث لدى حصولها. يمكن التخفيف من العملية التي تتطلب وقتاً وجهداً لاستخراج البيانات ذات الصلة والمفيدة من الكميّة الهائلة من المعلومات المنشورة على منصات وسائل التواصل الاجتماعي من خلال استخدام برمجيّات مصمّمة خصيصاً لفرز المنشورات ليتمكّن المحلّلون البشريون أو أنظمة التعلّم الآلي من إجراء هذه الأنواع

من التحليلات مباشرةً. تتوفر أصلاً البرمجيات التي يمكن أن تُجري تحليلاً لموثوقية المنشورات على وسائل التواصل الاجتماعي، وقد ساعدت في الحدّ من كميّة المعلومات التي ليس لها صلة بالموضوع والتي يتوجّب على المُستَخدِمين النهائيين البشريين تحليلها. وتَسْتَخْدِم هذه البرمجيات أيضاً تحليل المشاعر من أجل تحديد الحسابات المؤيدة للحكومة وتلك المعادية لها ويمكن أن ترسم خريطة للشبكات الاجتماعية للجانبين باستخدام هذه المعلومات (كايس وآخرون [Kase et al.]، 2014). ليست هذه البرمجيات قادرة حتّى الآن على تحليل التغريدات بحدّ ذاتها وتنشأ المشاكل عندما تواجه برامج الحاسوب فروقات دقيقة في اللغة والثقافة. على الرغم من ذلك، إنّها تحدّ من كميّة المعلومات التي يُطلب من ممارسي عمليات المعلومات مراجعتها، وتوفّر سياقاً أغنى للتحليل. يتوقع الباحثون إمكانية استخدام التعلّم الآلي من أجل إجراء تحليلٍ للمشاعر لحشود المُحتَجّين في المستقبل، مع قياس المزاج والنزعة إلى العنف في أيّ وقتٍ كان (أوماند [Omand]، بارتليت [Bartlett]، وميلير [Miller]، 2012).

استخدمت الحكومات وخصومها وسائل التواصل الاجتماعي بنجاحٍ من أجل رصد المعلومات الاستخباراتية حول المواطنين الفرديين والمجموعات التي تشكّل شبكات وجمعها على حد سواء. في حين كان مدى انخراط الولايات المتحدة في هذه النشاطات محدوداً، يمكن أن تكون المعلومات المُستقاة من وسائل التواصل الاجتماعي قيّمة جدّاً في إعداد الاستخبارات لساحة المعركة. في المراكز الحضريّة بالتحديد، تُعدّ وسائل التواصل الاجتماعي مصدراً مثالياً للمعلومات حول مجال عمليات. يمكن أن يوفّر تحليل شبكات وسائل التواصل الاجتماعي والتحليل النصّي رؤية حول الناحيتين الاجتماعية والثقافية لبيئة المعلومات ويحدّدان التغيّرات. ومع تحسّن تحليل المشاعر والمصداقية، ستزداد سرعة التطبيقات والمعلومات التي تجمعها وموثوقيتها.

عمليّات دعم المعلومات العسكريّة

استخدمت الحكومات والجهات الفاعلة غير الحكومية على حدّ سواء وسائل التواصل الاجتماعي بكثافة للتأثير على الرأي العامّ في مناطق الصراع. في البيئات التشغيليّة، لدى وزارة الدفاع الأمريكيّة (DoD) حاجة ومسؤوليّة من أجل الكشف عن جهود الدعاية التي يبذلها الخصوم والخصوم المحتملون ومكافحتها. أطلقت الولايات المتّحدة عدداً من هذه الحملات في الماضي، ولكنّ طبيعة وسائل التواصل الاجتماعي السريعة التحرّك تتطلّب تقنيّات مختلفة من أجل تحديد عمليات تأثير الخصوم ورصدها ومكافحتها بسرعة. وجدت الدراسات أنّ الرأي العام على تويتر (Twitter) يتطوّر ثمّ يستقرّ بسرعةٍ كبيرةٍ ليصبح بمثابة رأي مُهيمن، ما يُعطي الميزة الأكبر لمجموعاتٍ كبيرةٍ قادرةٍ على

تشكيل الرأي في مرحلةٍ مبكرة (كزيونغ [Xiong] وليو [Liu]، 2014). وجد البحث باستخدام محاكاة الحاسوب لعمليات التأثير الشخصي بين الأفراد أن تشكيل الرأي العام يجري بدفعٍ من "مجموعةٍ مهمّةٍ من الأفراد الذين يتمّ التأثير عليهم بسهولة" (واتس [Watts] ودودس [Dodds]، 2007)، ما يجعل وسائل التواصل الاجتماعي والسهولة التي تتيح تبادل المعلومات بها مصدراً مثالياً لنشر الأفكار. من الأساسيّ بالنسبة لوزارة الدفاع الأمريكيّة فهم مدى استخدام الحكومات والجهات الفاعلة غير الحكوميّة وسائل التواصل الاجتماعي للتأثير على الرأي العام، بالإضافة إلى نجاحها لدى القيام بذلك.

وسائل التواصل الاجتماعي وعمليّات التأثير

يتيح رصد شبكات وسائل التواصل الاجتماعي وتَقَدُّم المشاعر المُتغيّرة للمخططين العسكريين فرصةً ليفهموا بشكلٍ أفضل كيف وأين تعمل هذه الجهات الفاعلة من أجل التأثير على الرأي العام. يمكن أن تُثير هذه البيانات بعدئذٍ الجهود الرامية إلى مكافحة حملاتها، ولكنّها تكشف أيضاً عن القضايا التي يعتبرها الخصوم الأكثر أهميّة. تُعتبر وسائل التواصل الاجتماعي فريدةً من حيث قدرتها على نشر الصور بسرعة، على الرغم من أنّ هذه الصور تكون غالباً مُضلّلة أو يتم نشرها بدون سياق. يمكن أن تؤدي صورة وحيدة أو مقطع فيديو قصير دور جهازٍ قويّ من أجل تبديل كيفيّة تَصَوُّر العامّة لقضية. نجحت نسبياً مجموعات مثل الدولة الإسلامية في العراق والشام (ISIL) في الاستفادة من وسائل التواصل الاجتماعي على مستوى الأرض في سوريا، مُشَكِّلةً سرد الصراع والرأي العام من خلال تعميم صور مُتحيّزة ومُنَظَّمة تبدو أنّها مواد خام تمّ نشرها من قِبَل مُستَخدِمين فرديين (زيتزوف [Zeitzoff]، كيلي [Kelly] ولوتان [Lotan]، 2015). استخدمت الصين وروسيا على حدّ سواء وسائل التواصل الاجتماعي بنشاطٍ بهذه الطريقة في حملات واسعة النطاق ومُنسّقة. تستخدم الصين آلاف الأشخاص من أجل نشر دعاية مؤيّدة للحكومة والترويج لأجندة الحزب على لوحات رسائل ومدوّنات (درابو [Drapeau] وويلز [Wells]، 2009). وتدفع روسيا بالمثل المال لأشخاص من أجل نشر محتوى موالٍ للحكومة وانتقاد الخصوم في غرف الدردشة وأقسام التعليقات التابعة للمقالات الجديدة (خازان [Khazan]، 2013).

كُتِبَ الكثير عن استخدام وسائل التواصل الاجتماعي من قِبَل حزب الله وحركة حماس، باعتبار أنّ هاتين المجموعتين تتمتعان بمهارات محدّدة في مجال استخدام وسائل التواصل الاجتماعي من أجل صياغة السرديّات في مناطق الصراع. عندما أطلقت إسرائيل ضربةً جوّيةً ضدّ حزب الله خلال حرب 2006 في لبنان، قامت المجموعة بتنقيح صور الضحايا وعمّال الإغاثة لتجعل الهجوم يبدو على شكل إبادة جماعيةٍ بدلاً من هجومٍ عسكريٍّ بطبيعته (كيلير [Keller]، 2010). كان أيضاً استخدام وسائل

التواصل الاجتماعي للتأثير على الرأي العام جزءاً من استراتيجيّةٍ أكبر لإرغام قوّات الدفاع الإسرائيلي (Israel Defense Forces [IDF]) على الكشف عن خططها. تمّ وصف حملة حزب الله على وسائل التواصل الاجتماعي على أنّها "إنتاج من ترتيب حزب الله، مصمّم بدقّة من أجل إشعال [كما ورد] الشعور الدولي ضدّ إسرائيل وإرغام الإسرائيليين على القبول بوقف إطلاق النار الذي قد يُمكّن مجموعة الجهاد الإرهابيّة من كسب المزيد من الوقت من أجل التعافي من الهجمات الإسرائيليّة" (سبنسر [Spencer]، 2006). ومع قيام الجانبين بإطلاق حملات دعاية على وسائل التواصل الاجتماعي، ادّعى أفراد ومنظّمات غير حكوميّة، بما في ذلك هيومن رايتس ووتش (Human Rights Watch) ومنظّمة العفو الدوليّة (Amnesty International) حدوث انتهاكات لحقوق الإنسان من جانب قوّات الدفاع الإسرائيلي، داعيةً المجتمع الدولي لاتّخاذ إجراءات.

لا يؤدّي استبعاد المُراسلين الأجانب من مناطق الحرب إلّا إلى زيادة تأثير الحملات على وسائل التواصل الاجتماعي. خلال صراع غزّة عام 2006، حاولت إسرائيل إبقاء وسائل الإعلام بعيدةً عن منطقة العمليّات. وجدت وسائل الإعلام الدوليّة التي مُنِع مراسلوها من دخول المنطقة مدوّنةً تعود لخرّيجٍ جامعيٍّ حديثٍ من غزّة، وسرعان ما أصبحت مصدرهم الأوّلي للمعلومات حول الوضع المتطوّر على الأرض. كان سامح حبيب (Sameh Habeeb) يُحَدِّث مدوّنته يومياً ويمدّ وسائل الأخبار بالتقارير حول الإصابات، والهجمات والوضع العام في غزّة. انتهى الأمر بوسائل إعلام رئيسية مثل سي أن أن (CNN)، وهيئة الإذاعة البريطانية (بي بي سي) (BBC)، ولو موند (Le Monde) بالاعتماد على تقارير حبيب وقد أوردتها في برامج بثّها (جيلينسكي [Gilinsky]، 2009).

وتصرّف بالمثل مواطنون آخرون من غزّة بمثابة صحفيين مواطنين، مُستَخدِمين يوتيوب (YouTube)، وتويتر (Twitter) ومدوّنات لتبادل مقاطع الفيديو والصور من منطقة الصراع. ومع منع صحافيين دوليين من إعداد التقارير مباشرةً حول الوضع في غزّة، لم يبقَ أمام وسائل الإعلام سوى القبول بصورٍ كانت تفتقر للمحتوى أو كانت مصحوبة بادّعاءات لا يمكن التحقّق منها. استُخدِم عدد من هذه المنشورات من أجل تعزيز التقارير الفلسطينية حول الفظائع التي ارتكبتها قوات الدفاع الإسرائيلي.

للمساعدة في مكافحة تأثير هذه النشاطات، نظّمت إسرائيل فِرَقَها الخاصّة من المُراسلين الوطنيين، وعمّمت قوّات الدفاع الإسرائيلي مشاهد مُصوَّرة عن قصفها الجوّي على قناتها على يوتيوب (YouTube)، مُشَدِّدةً على أنّها كانت في حالة حربٍ مع حماس، وليس مع سكّان غزّة المدنيين. وأطلقت حماس أيضاً حملة معلومات، مع إحصاءات تتناقض مع تلك التي نشرتها قوّات الدفاع الإسرائيلي ومعلومات أخرى

تهدف إلى التأثير على الرأي العام الدولي (جيلينسكي [Gilinsky]، 2009). في بيئة المعلومات المعقَّدة هذه، قد يساعد تحليل وسائل التواصل الاجتماعي الحكومات في استباق متى وكيف سيتمّ استخدام عمليات التأثير، مُتيحاً لممارسي عمليّات المعلومات (IO) تَجَنُّب تعميم معلومات خاطئة وتيسير استجابات أسرع لدى نشر هذه المعلومات.

في المناطق ذات أهمية بالنسبة للولايات المتحدة، ليس الخصوم وحدهم هم الذين ينخرطون في عمليات التأثير؛ تستخدم المجموعات غير الحكوميّة، التي تحاول مكافحة التطرّف والعنف، وسائل التواصل الاجتماعي كذلك الأمر. فعلى سبيل المثال، أسّست عام 2008 مجموعة من الطلّاب في كولومبيا مجموعة على فيسبوك (Facebook) باسم "مليون صوت ضدّ القوّات المسلّحة الثوريّة الكولومبيّة (One Million Voices Against the FARC [Revolutionary Armed Forces of Colombia])"، مع نشر وثائق ومقاطع فيديو للرهائن المُحتجزين في ظروفٍ قاسية. تمّ اختيار الرواية من قِبَل وسائل الإعلام الدوليّة، ما دفع بستة ملايين شخص من حول العالم لتنظيم مسيرةٍ ضدّ القوّات المسلّحة الثوريّة الكولومبيّة (FARC) والضغط بنجاحٍ على المجموعة من أجل إطلاق سراح المزيد من الرهائن (جيندرون [Gendron]، بلاس-إيريزاري [Blas-Irizarry] وبوجس [Boggs]، 2009).

مع تنافس وسائل الأخبار على بثّ الأحداث قبل منافسيها، تعتمد على الحملات على وسائل التواصل الاجتماعي وتلفت الانتباه الدوليّ إلى هذه القضايا. بهذه الطريقة، تقترن صور فرد واحد بالقدرة الكامنة على التأثير على الرأي العام حول قضيّة من حول العالم. ثمّة حاجة واضحة إلى أدوات تحليلية من أجل رصد عمليات التأثير وآثار وسائل التواصل الاجتماعي على نطاقٍ واسع. قد تؤدي هذه التحليلات دور آلية قوّيّة للتحقّق من تقارير المُستَخدِمين وإنارة الاستجابات المناسبة.

الأهميّة الكبيرة لعمليات التأثير

لا يمكننا التشديد بما يكفي على أهميّة عمليّات التأثير بالنسبة لنجاح مهمّة. لكلّ شيء تقوم به وزارة الدفاع الأمريكيّة (DoD) — أو تُخفِق في القيام به — تأثيرٌ من الناحية التشغيليّة على بيئة المعلومات. ولأنّه من المرجّح الطعن بشكلٍ نشطٍ بعملٍ عسكريٍّ أمريكيٍّ عبر سلسلةٍ من العمليات من قِبَل الذين يعارضون المصالح الأمريكيّة، يتوجّب على القادة والمخطّطين العسكريين أن يأخذوا بعين الاعتبار تأثير وسائل التواصل الاجتماعي على الجماهير. تؤكّد الأمثلة التي يتمّ عرضها في هذا الفصل على أهميّة الرصد والتحليل الأمريكيين لعمليات التأثير من خلال وسائل التواصل الاجتماعي، ولكنّ الخلاصة المهمّة هي أنّ الدعم الشعبي يُشكّل غالباً جداً عاملاً رئيسياً في نجاح مهمّة. من خلال استخدام **تحليل** وسائل التواصل الاجتماعي لفهم كيفية استخدام الجهات الفاعلة

الحكوميّة والجهات الفاعلة غير الحكوميّة لوسائل التواصل الاجتماعي من أجل التأثير على الرأي العام فهماً أفضل، يمكن للقادة استباق الدعم المدني في ساحة المعركة وتشجيعه بشكلٍ أفضل، بالإضافة إلى تحديد القيود المحتملة على استخدام القوّة.

أمن العمليّات (OPSEC) والتضليل العسكري (MILDEC)

يُشكّل تأثير وسائل التواصل الاجتماعي على الأمن التشغيلي مصدر قلقٍ متنامٍ بالنسبة لوزارة الدفاع الأمريكيّة (DoD). تملك الوزارة والأقسام والوحدات والموظّفون الفرديون حسابات على فيسبوك (Facebook)، وتويتر (Twitter)، ويوتيوب (YouTube)، وسنابشات (Snapchat)، وإنستغرام (Instagram) ووسائل تواصل اجتماعي أخرى. تُسْتَخْدَم المواقع التي تديرها منظّمات عسكريّة أمريكيّة للتجنيد وتعميم المعلومات. في حين يُعتبر من غير المرجح أن تُسرّب هذه المواقع الرسميّة معلومات قد تقوّض أمن العمليّات (OPSEC)، قد يقوم عددٌ من العسكريين الذين ينخرطون مع هذه المنصّات بذلك بشكلٍ غير متعمّد. يقترن تحليل وسائل التواصل الاجتماعي بالقدرة الكامنة على دعم أمن العمليات والتضليل العسكري (MILDEC) من خلال الكشف عمّا إذا تمّ فضح مؤشرات مهمّة. فعلى سبيل المثال، في حال نَشَرَ عسكري صورةً لخليج صيانة يعجّ بالطائرات، فهو (أو هي) قد يوفّر (توفّر) عن غير قصد مؤشّراً مهماً على الجهوزية. ويعتبر الكشف عن مثل هذه الانتهاكات أمراً مهمّاً من أجل المحافظة على أمن العمليات. بالمثل، ثمّة تطبيقات للتضليل العسكري بالنسبة لتحليل بيانات وسائل التواصل الاجتماعي على نطاقات مختلفة: قد تُحذّر بيانات وسائل التواصل الاجتماعي التي يتم الحصول عليها من الخصوم أو الشعوب المحليّة القادة بأنّه يتم تقويض عملية التضليل التابعة لهم.

وجدت دراسة أُجريت عام 2011 وربطت بين سجلات وزارة الدفاع الأمريكية (DoD) الرسميّة وأدلّة على مواقع وسائل التواصل الاجتماعي أنّ بين 25 و57 في المئة من موظفي وزارة الدفاع الأمريكية كانوا يملكون حسابات على فيسبوك (Facebook) (فيليبس [Phillips] وبيكيت [Pickett]، 2011). لوحظ استخدام منصات وسائل التواصل الاجتماعي المنتشر على نطاقٍ واسع، جنباً إلى جنب مع سهولة تحديد العسكريين وعائلاتهم، من قِبَل مجموعات إرهابيّة أصدرت تعليمات إلى عناصرها من أجل رصد أفراد على هذه الشبكات واستهدافهم.

يستخدم الخصوم الأمريكيون بشكلٍ شبه مؤكَّد وسائل التواصل الاجتماعي من أجل جمع المعلومات الاستخباراتيّة. يتبع حساب حركة طالبان على تويتر (Twitter) حسابات موظّفين عسكريين أمريكيين متعدّدين. دعت الدولة الإسلامية في العراق والشام (ISIL) عام 2014 الأتباع لاستخدام مواقع على وسائل التواصل الاجتماعي مثل "دليل الصفحات

الصفراء" على الإنترنت من أجل جمع المعلومات الشخصية للعسكريين، بما فيها عناوين سكنهم (ليفين [Levin]، 2015). يمكن أن يساعد رصد هذا النوع من نشاط الخصوم المسؤولين الاستخباراتيين ليقيسوا بشكلٍ أفضل المعلومات المُتوفّرة على وسائل التواصل الاجتماعي حول المواطنين الأمريكيين ومدى مراقبة الخصوم لهذه المواقع. ويمكن أن تستخدم وزارة الدفاع الأمريكية هذه المعلومات بشكلٍ إضافيٍّ من أجل توجيه الجهود الوقائية بشكلٍ أكثر دقّة وحماية البيانات الحساسة.

إن عدم الكشف المُتصوّر عن الهوية على الإنترنت وسهولة تأسيس حسابات على وسائل التواصل الاجتماعي يجعلان منها مكاناً مثالياً لتضليل الأفراد وعامة الجمهور على حدّ سواء. ويوفّر أيضاً عددٌ من استراتيجيات جمع المعلومات الاستخباراتيّة المحدّدة في هذا الفصل فرصاً للتضليل. ويتيح جمع كميات كبيرة من بيانات وسائل التواصل الاجتماعي وفرزها من قِبَل الحواسيب على سبيل المثال الفرصة لمجموعات الخصوم لغَمْرِ نظامٍ بمعلومات مُضلّلة عمداً.

تحديد المعلومات المضلّلة بسرعة

يمكن تسخير قدرة وسائل التواصل الاجتماعي على نشر المعلومات المُضلّلة بسرعةٍ من قِبَل جهات فاعلة خبيثةٍ للتشجيع على العنف وإثارة الذعر. غالباً ما يتمّ نشر الروايات الخاطئة والإشاعات على وسائل التواصل الاجتماعي، لا سيّما بعد هجمات إرهابية كبيرة. وقد تمّ حتّى اختيار بعض هذه الروايات عن غير قصدٍ من قِبَل وسائل الأخبار الرئيسية. قد يتيح رصد وسائل التواصل الاجتماعي وتحليلها للحكومات أن تحدّد وتكافح بسرعةٍ أكبر انتشار المعلومات الخاطئة. وبالتحديد، قد يستفيد قادة المقاتلين من تحليل وسائل التواصل الاجتماعي لبيئة المعلومات في المنطقة الجغرافية حيث تقع مسؤولياتهم.

بعد أن أدّت اشتباكات بين الهندوس والمسلمين إلى إعادة استيطان 300,000 لاجئ مسلم في مُخيّمٍ خاضعٍ للحراسة في آسام، الهند، عام 2012، أبلغ المسلمون في مناطق حضريّة مجاورة عن تعرّضهم للمضايقات والهجمات من قِبَل الهندوس. وبعد فترةٍ وجيزة، بدأت التقارير الخاطئة حول الهجمات والاشتباكات المستمرّة بالانتشار على وسائل التواصل الاجتماعي. أظهرت المنشورات على فيسبوك (Facebook) صوراً مُغيّرة ومقاطع فيديو مُنقّحة لأعمال الشغب والقتل الجماعي التي يُزعم أنّها من آسام؛ في الواقع، كانت قد التُقِطت بعد كارثةٍ طبيعيّة في التبت (Tibet) وميانمار (Myanmar). أثارت الصور ذعراً جماعياً واحتشد المسلمون في محطّات القطار وملأوا مخيّمات اللاجئين. تفاقمت الأزمة بسبب المسؤولين عن إنفاذ القانون غير المُستعدّين والذين كانوا غير قادرين على رصد انتشار حملة المعلومات المُضلّلة وتأثيرها. اكتشفت السلطات الهنديّة في وقتٍ لاحقٍ أنّ عدداً قليلاً فقط من الناس قد شنّوا الهجمات، مع

إرسال فردٍ واحدٍ 20,000 رسالة من الرسائل المُضلّلة (جولسبي [Goolsby]، 2013). مكّنت وسائل التواصل الاجتماعي الانتشار السريع للصور، مؤدّيةً إلى استجابةٍ مُسْرِعَة من الشرطة على التدفّق المفاجئ للاجئين. شكّلت السهولة التي تمكّن بها عددٌ قليلٌ من الأفراد من إثارة ذعر منتشر على نطاق واسع تهديداً خطيراً لأمن الدولة. قد يحول رصد نشاط وسائل التواصل الاجتماعي دون حصول هذه الحوادث أو قد يسمح بأوقات استجابة أسرع من قِبَل وكالات إنفاذ القانون.

استخراج التفاصيل الحسّاسة من المعلومات المُتاحة للعامّة

يقترن تحليل وسائل التواصل الاجتماعي بالقدرة الكامنة على تحديد مخاطر أمن العمليّات (OPSEC) الناتجة عن الإفصاح عن المعلومات المُحدِّدة للهويّة الشخصيّة. لغاية عام 2011، كان من الممكن العثور على الأرقام الأربعة الأخيرة من رقم الضمان الاجتماعي التابع لعسكري على مواقع إلكترونيّة عامةّ (فيليبس [Phillips] وبيكيت [Pickett]، 2011). في حين يبدو هذا الأمر غير ضارّ، يمكن أن يكون الكشف للعامّة عن كميّاتٍ صغيرةٍ من المعلومات الحسّاسة كافياً لتشكيل ملفّ شخصيّ أكبر لهدف، مُتيحاً الفرصة أمام جهة فاعلة خبيثة لربط هذه التفاصيل بأفراد واستغلال هذه المعرفة من أجل الكشف عن هويّة موظّفي وزارة الدفاع الأمريكيّة (DoD) والعسكريين وتقويض أمنهم. إنّ إدخال بعض المعلومات الرئيسيّة بشأن فردٍ واحدٍ في محرّك بحثٍ قد يوفّر إمكانية الوصول إلى عناوين السكن، وأرقام الهاتف، ومعلومات حول أفراد العائلة. ويمكن أن توفّر تفاصيل إضافية متوفرة على صفحات وسائل التواصل الاجتماعي إجابات عن "أسئلة سرّيّة" للوصول إلى صفحات الحساب ومعلومات أساسيّة أخرى. قد يساعد مجرّد البحث عن العضويّة في مجموعات فيسبوك (Facebook) المرتبطة بوحدات عسكرية الخصوم في تحديد العسكريين المرتبطين بالوحدات وشبكاتهم الشخصية. في الوقت الذي أضحت فيه برمجيّات التعرّف على الوجه أكثر تقدّماً، أصبح من الممكن استخدامها من أجل ربط صور عسكرية رسمية مع الصور الشخصية للعسكريين وصفحاتهم على وسائل التواصل الاجتماعي.

الكشف عن معلومات حسّاسة في المنشورات على وسائل التواصل الاجتماعي

يُطلب من العسكريين وعائلاتهم مراراً عدم نشر معلومات حسّاسة، على غرار تواريخ النشر ومواقعه، على وسائل التواصل الاجتماعي، ولكنّه من المستحيل حالياً بالنسبة لوزارة الدفاع الأمريكية (DoD) رصد هذا العدد الكبير من الحسابات على وسائل التواصل الاجتماعي. على الرغم من ذلك، قد يكون استخدام مقاربة ممكننة أو يتحكّم بها الإنسان لرصد هذه الحسابات بحثاً عن معلومات حسّاسة قيّماً جداً من منظور أمن

العمليات (OPSEC). تتضاعف طلبات رصد حسابات فريق عمل حاملة طائرات يتألّف من 5,000 فرد على وسائل التواصل الاجتماعي عندما يُعهد للأصدقاء وأفراد العائلة بمعلومات حول أحبائهم. مع قيام العسكريين بنشر صور وتحديثات وقيام أفراد العائلة بتبادل المعلومات، يظهر خطرٌ متزايدٌ بأن تفشل الضوابط المفروضة على الخصوصية أو أن يتبادل مُستَخدِم معلومات حسّاسة مع جهةٍ فاعلةٍ خبيثة.

حصلت حالاتٌ متعدّدةٌ حيث قوّضت المنشورات على وسائل التواصل الاجتماعي أمن العمليات. أُرغمت عام 2010 قوات الدفاع الإسرائيلي (IDF) على تأجيل عمليّة بعد أن نشر جنديّ موقع الغارة المُخطَط لها ووقتها على صفحته الشخصية على فيسبوك (Facebook) (كاتز [Katz]، 2010). قام عام 2009 النائب بيتر هويكسترا (Representative Peter Hoekstra)، وهو عضو في لجنة الاستخبارات التابعة لمجلس النواب (House Intelligence Committee)، بالتغريد بموقعه ونشاطاته كل بضع ساعات وهو في رحلة حسّاسةٍ إلى العراق، مُعّرضاً نفسه ورفقائه في السفر للخطر (ليفين [Levin]، 2015).

ظهرت إضافة الوسم الجغرافي بمثابة تهديد خطير بشكلٍ خاصّ بالنسبة لأمن العمليات، علماً أنّ عدداً من المُستَخدِمين لا يدركون أنّ الوسوم الجغرافيّة تكون مُضمّنة آلياً في الصور التي يتم التقاطها باستخدام الأجهزة الجوالة. بالعودة إلى مثالٍ تمّ ذكره سابقاً، أثبت الجنرال في القوى الجويّة هربرت "هوك" كارلايل (Air Force General Herbert "Hawk" Carlisle) مؤخراً الفائدة الهائلة للمنشورات على وسائل التواصل الاجتماعي والتي تحمل وسماً جغرافياً عندما ضبطت وحدته موقع مبنى مقرّ رئيسي تابع للدولة الإسلامية في العراق والشام (ISIL) بالاعتماد على منشور يحمل وسماً جغرافياً لمقاتل تابع للدولة الإسلامية في العراق والشام. دمّرت الوحدة الهيكلية بثلاث ذخائر هجوم مباشر مشترك بعد 22 ساعة فقط (إيفرستاين [Everstine]، 2015). بالعكس، يمكن أن تتسبّب الصور أو المنشورات على وسائل التواصل الاجتماعي والتي تحمل وسماً جغرافياً بخطرٍ بالنسبة للقوات الأمريكية من خلال الكشف عن مواقع الوحدات وأنماط التحرك في منطقة صراع وفي الداخل على حدّ سواء.

يُعتبر الوعي حول توفّر المعلومات المُتاحة للعامّة وأساليب تجنّب انتشارها مهمّاً لحماية العسكريين وأمن العمليات. يمكن أن يحسّن تدريب العسكريين الذي يعتمد على نتائج تحليل وسائل التواصل الاجتماعي ممارسات أمن العمليّات ويعزّز فهم العسكريين للسهولة التي يمكن استنتاج المعلومات الشخصية بها من المنشورات. على مستوى تنظيمي، يمكن أن ينير هذا النوع من التحليل الجهود الوقائية الخاصّة بوزارة الدفاع الأمريكيّة بشكلٍ أفضل.

الشؤون العامّة

كافحت وزارة الدفاع الأمريكيّة (DoD) لتحقيق التوازن بين المطالبات بشأن عمليات المعلومات (IO) وحاجات الشؤون العامّة، بحيث ذهبت بعيداً لدرجة إغلاق مكتب التأثير الاستراتيجي (Office of Strategic Influence) التابع لها بعد أن اتّهمتها مقالة نُشرت في نيويورك تايمز *(New York Times)* بـ"محاولة التأثير على الجمهور الأمريكي" (أوبرمان [Opperman]، 2012). وعلى الرغم من ذلك، كما يتضح من أمثلةٍ سابقةٍ في هذا الفصل، بقيت قدرة الخصوم على نشر المعلومات والدعاية بسرعةٍ آخذةً بالزيادة.

على الرغم من أنّ وزارة الدفاع الأمريكية عمِلت لتنفيذ استراتيجيّاتها الخاصّة بوسائل التواصل الاجتماعي دعماً لحملات الشؤون العامّة، يستدعي استخدام خصوم الولايات المتحدة المستمرّ لوسائل التواصل الاجتماعي قيامها بتوسيع هذه الاستراتيجيّات لتمكينها من تعقّب المعلومات حول نشاطات الخصوم وجمعها. أثبتت حملات المعلومات المتنافسة لقوّات الدفاع الإسرائيلي (IDF)، وحماس وحزب الله الارتباك الذي يمكن أن يحصل عندما تترافق صراعات عسكريّة مع معركةٍ لهيمنة المعلومات على منصّات وسائل التواصل الاجتماعي. بالمثل، يكشف انتشار التقارير الخاطئة حول العنف ضدّ المسلمين بالقرب من آسام في الهند عن السهولة التي يمكن أن يؤثّر بها عددٌ صغيرٌ من الأفراد على التصوّرات وأن يعزّز هذا النوع من الارتباك. غالباً ما يتمّ تصنيف جهود الشؤون العامّة التي تبذلها المجموعات الإرهابية على أنّها "دعاية"، ولكنّ هذه المجموعات تكرّس وقتاً وموارد هائلة من أجل تعميم المعلومات، والرسائل والوسائط المتعددة. في بعض الحالات، استخدمت الشبكات الإعلامية التقليدية، التي تفتقر إلى إعداد التقارير المباشرة الخاصّة بها، مقاطع فيديو من إنتاج مجموعات إرهابية في عمليات البثّ الخاصّة بها، وذلك غالباً بدون إخلاء مسؤوليّة لتحديد المصدر (دوبير [Dauber]، 2009).

قد تحدّ استراتيجيّة مرنة واستباقيّة بشكلٍ أكبر للشؤون العامّة خاصّة بوزارة الدفاع الأمريكية من تأثير حملات الخصوم هذه. من منظورٍ يتمحور حول وزارة الدفاع الأمريكية، تتمتّع المنظّمات المعنيّة بالشؤون العامّة بموقعٍ جيّدٍ من أجل إنارة جهود تحليل وسائل التواصل الاجتماعي الموجّهة نحو أمن العمليات (OPSEC) أو حماية القوّات. يمكن أن يساعد رصد استخدام دعاية العدو من خلال تحليل وسائل التواصل الاجتماعي لحصر كيف ومتى وأين يتم نشرها في توجيه جهود الشؤون العامّة بطرقٍ أكثر آنية وفعالية. وقد يكشف أيضاً عن الأماكن التي تفتقر فيها وسائل الإعلام التقليديّة إلى التغطيّة، ما يحدّ من الاعتماد على مراقبين غير موثوقين أو متحيّزين للحصول على تقارير من مناطق الصراع. بالنظر إلى أنّ منظّمات الشؤون العامّة التابعة لوزارة الدفاع الأمريكية تنشط في الفضاءات الرقميّة، مثل تشغيل مجموعات الجهوزيّة على وسائل التواصل الاجتماعي، وأنّه يجب دمجها في عمليات المعلومات بشكلٍ واضح، قد تستفيد

إمكانية وصول المسؤولين عن الشؤون العامّة إلى الأدوات والأساليب التحليلية من هذه الجهود بقوّة.

العمليّات المدنيّة-العسكريّة

جرى القليل من البحث حول استخدام وسائل التواصل الاجتماعي دعماً للعمليّات المدنيةّ–العسكريّة، ولكن يقترن تحليل وسائل التواصل الاجتماعي بقدرة كامنة كبيرة على إنارة هذه الجهود والاستفادة منها. تبنّت منظّمات المعونة الإنسانيّة وسائل التواصل الاجتماعي باعتبارها أداةً لتحسين عمليّاتها. يمكن نقل عددٍ من أساليبها إلى بيئة صراع. جنّدت أوبن ستريت ماب (خريطة الطريق المفتوحة) (OpenStreetMaps)، وهي كناية عن مجموعة مفتوحة المصدر مخصصة لتطوير خريطة مفصلّة للعالم، متطوّعين من أجل إنشاء تخطيطات لأحياء هايتي التي لم يتم رسم خرائط لها مسبقاً وتبادلها ليستخدمها عمّال الإغاثة (نيلسون [Nelson]، 2011). تم استخدام فيسبوك (Facebook) وغيره من منصّات وسائل التواصل الاجتماعي من أجل رسم "خرائط الأزمات"، مُنبّهةً عمال الإغاثة حول المناطق التي تحتاج إلى المساعدة (جولسبي [Goolsby]، 2013). وفّر استخدام وسائل التواصل الاجتماعي من أجل الإبلاغ عن الإصابات وتصنيف الوضع على الأرض لمنظّمات الإغاثة المعلومات اللازمة لاستجابةٍ آنيةٍ في أعقاب الزلزال والتسونامي اللذين ضربا اليابان عام 2011 (عباسي وآخرون [.Abbasi et al]، 2011). وتوفّر تويت تراكر (TweetTracker)، وهي أداة تستخدم واجهة برمجة التطبيقات (Application Programming Interface [API]) الخاصّة بتدفّقات تويتر (Twitter) من أجل استرجاع التغريدات وتخزينها وتحليلها، تحليلاً قيّماً لعمليّات المساعدة الإنسانيّة/الإغاثة في حالات الكوارث (كومار وآخرون [.Kumar et al]، 2011). تشمل ميزاتها تجسيدات مرئيّة تفاعليّة للتغريدات المحدّدة الموقع الجغرافي حول مواضيع ذات أهميّة، بالإضافة إلى ملخّصات البيانات، وخيارات الترجمة، وتعقّب الاتجاهات ومقارناتها.

قد يساعد بُعدا تبادل المعلومات والمصادر الخارجيّة لوسائل التواصل الاجتماعي القادة في استهداف مجتمعات أو مناطق محددة لجهود الاتصالات المدنية–العسكريّة خلال عمليات مكافحة التمرّد. قد يستكمل رصد وسائل التواصل الاجتماعي أيضاً نشاطات الاتصالات وجهاً لوجه مع تقدّم هذه العمليات. باستخدام خرائط الأزمات، وتحليل مشاعر العامّة، وأنواع أخرى من جمع بيانات وسائل التواصل الاجتماعي وتحليلها، قد يقيس القادّة ومخططو فريق العمل فعالية حملات معلومات محدّدة أو عمليّات مدنية–عسكرية وتأثيرها بشكلٍ أوسع.

انخراط القادة الرئيسيين

كافحت وزارة الدفاع الأمريكية (DoD) لتطوير سياسات تشجّع على استخدام وسائل التواصل الاجتماعي مع المحافظة على أمن العمليات (OPSEC). جعل هذا النقص في التوجيه القادة يتردّدون في استخدام وسائل التواصل الاجتماعي، متيحاً بالتالي للمجموعات الإرهابية التي تملك دراية في وسائل التواصل الاجتماعي أن تنشر أفكارها وسردياتها، وغالباً بدون حملات معلومات مضادّة كبيرة من قِبَل الولايات المتحدة. وصف تيموثي كونينجهام (Timothy Cunningham)، وهو نائب مدير برنامج في مركز المصدر المفتوح التابع لمدير الاستخبارات القومية (Director of National Intelligence Open Source Center)، المشكلة على أنّها متجذّرة في اعتماد وزارة الدفاع الأمريكيّة (DoD) على وسائل الإعلام القديمة وتدفّق المعلومات الأحادي الاتجاه الخاص بها بدلاً من الاستفادة من الطبيعة التفاعليّة لوسائل الإعلام الجديدة (شوين [Schoen]، 2011).

وكما هي الحال بالنسبة لعمليات دعم المعلومات العسكرية (MISO)، نعتقد أنّ المقاربات التحليليّة الخاصة بوسائل التواصل الاجتماعي تقترن بقدرةٍ كامنةٍ هائلةٍ على إنارة انخراط القادة الرئيسيين. في الفصل الثالث، نحدد بعض المقاربات التي قد توفّر للقادة أسلوباً فعّالاً للحصول على رؤية حول الشعور العامّ ومخاوف الشعوب المحلية، بالإضافة إلى الكشف عن استراتيجيات الحُجَج التي يتم تداولها من قِبَل المؤثّرين الرئيسيين وفيما بينهم وتفريغها. قد يساعد هذا النوع من التحليل الذي ينطلق من القاعدة نحو الأعلى بدفعٍ من البيانات القادة لتجنّب "عكس" الأخطاء في التواصل وتطوير استراتيجيات إشراكٍ ستلقى صدى لدى القادة الرئيسيين.[1]

إطار عمل مرتكز إلى القدرات المرتبطة بالمعلومات (IRC) لبناء القدرة التحليلية الخاصة بوسائل التواصل الاجتماعي

بدأ هذا الفصل بمناقشة المفاهيم القابلة للتعميم بشكلٍ كبير، مقترحاً إطار عمل مرتكز إلى القدرات المرتبطة بالمعلومات (IRC) لدمج تحليلات بيانات وسائل التواصل الاجتماعي وعمليات المعلومات (IO). وفّرت المناقشة اللاحقة توجيهاً نحو بعض التطبيقات التشغيليّة للأدوات التحليلية، مرفقاً بأمثلة ولمحات موجزة حول المنافع والمخاطر المحتملة. يستكشف الفصل الثالث فائدة تحليل وسائل التواصل الاجتماعي بتحديدٍ أكبر، مُقدّماً مجموعة توضيحيّة من المقاربات المنهجيّة لحلّ مشاكل معيّنة مرتبطة بعمليات المعلومات

[1] يشير "العكس" إلى إسقاط القيم والأهداف والمعايير على جمهور مُستهدف.

باستخدام بيانات وسائل التواصل الاجتماعي.

يقدّم الجدول رقم 2.2 لمحة حول المقاربات المنهجية التي تنطبق على كلّ قدرة مرتبطة بالمعلومات، بما فيها تحليل الشبكات الاجتماعية (Social Network Analysis [SNA])، تحليل فئات العامّة، والتحليل اللغويّ، وتحليل الموقف، وتحديد الموقع الجغرافي والاستدلال الجغرافي، والشبكات العصبية العميقة ([deep neural networks [DNN). يناقش الفصل الثالث هذه المقاربات وكيفيّة التمكّن من تطبيقها بتفصيل أكبر. ويُعتبر عدد من هذه المقاربات أكثر قيمة بعد لدى استخدامها جنباً إلى جنب مع مقاربات أخرى. وكما ذُكر سابقاً، يقترن منشور على وسائل التواصل الاجتماعي يُظهر خليج صيانة يعجّ بالطائرات بالقدرة الكامنة على إلحاق ضرر خطير بأمن العمليات (OPSEC). إن استخدام الشبكات العصبية العميقة من أجل تحديد أنواع الطائرات آلياً في الصور وتحديد الموقع الجغرافي من أجل تحديد أين تم التقاط الصورة قد يساعد القادة في تحديد معلومات حساسة وتجنّب انتشارها العرضي. ومع تطوّر استخدام وسائل التواصل الاجتماعي، ستصبح مقاربات متنوعة أقلّ أو أكثر قيمة بالنسبة لبعض القدرات المرتبطة بالمعلومات المعيّنة.

الجدول رقم 2.2
القدرات المرتبطة بالمعلومات (IRCs) والمقاربات المنهجية

القدرة المرتبطة بالمعلومات (IRC)	المقاربات المنهجية القابلة للتطبيق
الاستخبارات	تحليل الشبكات الاجتماعية (SNA)، التحليل اللغوي، تحليل الموقف، تحديد الموقع الجغرافي، الشبكات العصبية العميقة (DNN)
عمليات دعم المعلومات العسكرية (MISO)	تحليل فئات العامّة، التحليل اللغويّ، تحليل الموقف، تحديد الموقع الجغرافي
أمن العمليات (OPSEC) والتضليل العسكري (MILDEC)	تحديد الموقع الجغرافي، الشبكات العصبية العميقة (DNN)
الشؤون العامّة	تحليل فئات العامّة، التحليل اللغويّ، تحليل الموقف
العمليات المدنية–العسكرية	تحليل فئات العامّة، التحليل اللغويّ، تحليل الموقف، تحديد الموقع الجغرافي
انخراط القادة الرئيسيين	تحليل فئات العامّة، التحليل اللغويّ، تحليل الموقف

أساليب الدراسات التحليلية حول وسائل التواصل الاجتماعي لدعم عمليات المعلومات

في الفصل السابق، عرضنا إطار عمل مرتكزاً إلى القدرات المرتبطة بالمعلومات (IRC) للتفكير في المنافع المحتملة لتطبيق تحليل وسائل التواصل الاجتماعي على عمليات المعلومات (IO). في هذا الفصل، ننتقل إلى مجموعة محدّدة بشكلٍ أكبر من التوضيحات: المقاربات المنهجيّة لقياس القبول الشعبي لدعاية مجموعة متطرّفة، وتحديد المخاوف الثقافيّة أو الإقليميّة دعماً لاستراتيجيات الرسائل، وحلّ مشاكل أخرى مرتبطة بعمليات المعلومات. لا يركّز هذا الفصل على تكنولوجيّات أو خوارزميّات محدّدة حيث يمكن أن تصبح مناقشات **الأساليب** هذه بالية بسرعة. بدلاً عن ذلك، نستكشف بعض **الطرق** الواعدة لمعالجة تحدّيات عمليات المعلومات الشائعة ضمن إطار عمل مألوف. على سبيل المثال، يمكن استبدال الخوارزميات الكاشفة للمجموعات الشائعة، مثل كلوزيت–نيومان مور (Clauset–Newman Moore)، بخيارات متفوّقة، ولكن تبقى الحاجة قائمة لتمييز المجموعات وتحليلها ضمن شبكةٍ اجتماعيّةٍ قائمة.

محدوديّات وسائل التواصل الاجتماعي بوصفها مصدر بيانات

تقترن بشكلٍ ممكنٍ المفاهيم والمقاربات التي شملتها الدراسة الاستقصائيّة في هذا الفصل بقيمة هائلة بالنسبة لوزارة الدفاع الأمريكية (DoD)، ولا شكّ في أنّ وسائل التواصل الاجتماعي هي مصدر بيانات مهمّ لعمليّات المعلومات (IO). على الرغم من ذلك، ثمّة بعض المحدوديّات للاستفادة من منصّات وسائل التواصل الاجتماعي والأدوات التحليليّة:

- يختلف معدّل تغلغل وسائل التواصل الاجتماعي من حول العالم، وينعكس ذلك في كميّة البيانات المتوفرة للتحليل (وقابليّة تطبيقها) في مجال عمليّات محدّد.
- ليست بيانات وسائل التواصل الاجتماعي تمثيليّة. يختار المشاركون أنفسهم، وبالتالي، تميل البيانات التي يتبادلونها نحو المجموعات التي تشارك.

ولذلك، على سبيل المثال، يكشف تحليل بيانات تصنيف الصور الممكنن المستمدّة من صور متبادلة على وسائل التواصل الاجتماعي عن الأمور التي تعتقد مجموعة فرعيّة من المجموعات أنّها تستحق أن يتم تبادلها.

المفاهيم والأساليب الرئيسية في تحليل وسائل التواصل الاجتماعي

ليست التحليلات النموذجية التي تلي شاملة، ولكن تم اختيارها لإظهار مجموعة المقاربات الممكنة ولتوضيح قيمة المقاربات المشتركة التي تستخدم أساليب تحليليّة متعدّدة. وفي حين تستخدم أغلبية المقاربات التحليل النصّي (ما يعكس وفرة البيانات المرتكزة إلى النصوص في وسائل التواصل الاجتماعي)، أدرجنا أيضاً أمثلة تنطوي على تحليل الشبكات، والتحليل الجغرافي–المكاني، وتحليل الصور.

تشمل المفاهيم المنهجية الرئيسيّة في هذا الفصل ما يلي:

- **تحليل الشبكات الاجتماعية** *(Social Network Analysis)*. تحليل الشبكات الاجتماعيّة (SNA) الذي ينطوي على تحديد الهيكليات الاجتماعيّة وتجسيدها مرئياً، يعتمد على العمل في مجالات عِلم النفس، وعِلم الإنسان (الأنثروبولوجيا) ونظرية الرسم البياني في الرياضيات (سكوت [Scott]، 2012). يشمل خوارزميّات الكشف الممكنن عن المجموعات في مجموعات واسعةٍ من بيانات وسائل التواصل الاجتماعي.
- **فئات العامّة**. فئات العامّة هي وحدة تحليل في الإقناع العام: أفكار مُستخلَصة لأشخاص لديهم مصلحة تحقيق التأييد، باستخدام لغة مُشتركة من أجل معالجة مشكلة شائعة. وتشكّل الرابطة الوطنية لحملة البنادق في أمريكا (National Rifle Association) مثالاً من العالم الحقيقي حول منظّمة مَعْنِية بالتأييد، ولكنّ العامّة التي تستخدم لغة مماثلة وتتشاطر هدف شرعنة الملكيّة الخاصّة للأسلحة هي استخلاصٌ أكبر بكثير. وتُعتبر العامّة المعارضة التي تسعى إلى الحدّ من ملكية الأسلحة أكبر أيضاً من أي جماعة ضغط رسميّة. يركّز هذا النوع من التحليل على مجموعة الأشخاص الذين يهتمّون بقضية ويستخدمون خطاباً مشتركاً للتأثير على النقاش.
- **التحليل اللغويّ**. تم تطوير مقاربات التحليل النصّي في دراسات عِلم لغة المدوّنة الحاسوبية.[1] يستخدم التحليل اللغويّ اختبارات إحصائية من أجل عدّ تواتر الكلمات،

[1] عِلم لغة المدوّنة الحاسوبية (Corpus linguistics) هو اختصاص فرعي من اللغويات، يتميّز بإجراء دراسة

والمسافة بين الكلمات، وخصائص أخرى من أجل الكشف عن الهيكلية والأنماط في البيانات النصيّة. يُستخدم بالشكل الأكثر تكراراً من أجل تحديد ما هو تجميع النصوص من الناحية التجريبية، وذلك من خلال الوجود المفرط أو القليل للكلمات بشكلٍ واضح، ووصلات الكلمات.

- **تحليل الموقف**. باعتباره نوعاً أكثر تطويراً وتفصيلاً من تحليل المشاعر، ينظر تحليل الموقف في تواتر **فئات** من الكلمات والتعابير (مثل: الغضب، الحزن، المستقبل، الماضي، اليقين، عدم اليقين). إنّه مفيد للإجابة عن الأسئلة الاجتماعية الثقافية حول المواقف والعواطف والقيم.
- **تحديد الموقع الجغرافي والاستدلال الجغرافي**. هذان أسلوبان خاصّان بالجغرافيا لتحديد الأصل الجغرافي لرسالة على وسائل التواصل الاجتماعي. يستخدم تحديد الموقع الجغرافي وسم النظام العالميّ لتحديد المواقع (GPS) وهو غاية في الدقّة؛ على الرغم من ذلك، غالباً ما يوقف المُستَخدِمون تشغيل هذه الميزة. يمكن أن يلتقط الاستدلال الجغرافي عيّنةً أكبر من البيانات من خلال استخدام البيانات الوصفيّة للاستدلال على الموقع الجغرافي للناشرين، وتتمتّع بعض الأساليب بمستويات عالية من الدقّة.
- **الشبكات العصبيّة العميقة** *(Deep neural networks)* الشبكات العصبية العميقة (DNNs) تتيح للآلات تعلّم مهام التصنيف من خلال تبسيط الاستخلاصات المُعقَّدة إلى طبقات. فعلى سبيل المثال، في حين قد ينظر فردٌ إلى صورةٍ ويرى دبّابة بشكلٍ كلي، من الممكن أن تكون قد تمت برمجة مُصنّف الصور الخاص بالشبكات العصبية العميقة للتمييز بين البنية المعدنية، وأشكال السطح الخارجي، وشكل رئيسي لبندقة، وقيمة انعكاسية منخفضة، وعوامل أخرى لتصنيف "دبابة" بمستوى معقول من الدقّة. بدلاً من أن يمضي محلل بشري سنة للبحث في مئات آلاف الصور، قد يتطلّب نموذج للشبكات العصبية العميقة يتم التدريب عليه جيداً مع قوة حوسبة جيدة أياماً فقط من أجل تصنيف المجموعة نفسها من الصور.

المقاربات لتحليل بيانات وسائل التواصل الاجتماعي

في حين تشمل بيانات وسائل التواصل الاجتماعي بشكلٍ متزايدٍ صوراً ومقاطع صوتيةً

تجريبيّة لمجموعات واسعة جداً من البيانات النصيّة *(Corpora)*. وبما أنّ عِلم لغة المدوّنة الحاسوبيةّ يرتكز إلى الآلة، فهو يفتقر إلى الدقّة والحساسية للسياق الخاصتين بالتحليل البشري، غير أنّ التحليل البشري لا يستطيع أن يضاهي قابلية توسّعها وموثوقيتها.

ومقاطع فيديو، لا تزال البيانات النصيّة مُهَيْمِنَة. في الأقسام التالية، نراجع مقاربات تحليلية مختلفة خاصّة بوسائل التواصل الاجتماعي — وبشكلٍ خاص تلك التي تستخدم البيانات النصيّة — والتي يمكن تطبيقها في العالم الحقيقي في مجال حلّ المشاكل المرتبطة بعمليات المعلومات (IO). يلخّص الجدول رقم 3.1 المقاربات التي تتم مناقشتها في هذا الفصل والتطبيقات النموذجية.

وصف الشبكات: الكشف عن شبكات المتطرفين على وسائل التواصل الاجتماعي

في حين يركّز هذا الفصل في المقام الأوّل على الأساليب التحليلية، نلاحظ القيمة في العمل الوصفي الذي قد يوفّر رؤية مهمّة من خلال الاستدلال. يفصّل هذا القسم أسلوباً لتمييز شبكات المتطرفين — وبالتحديد أفراد الشبكة الذين ينخرطون بشكلٍ نشطٍ في نشاطات الدعم.[2] في هذا المثل، كان الهدف وصف المناصرين النشطين للدولة الإسلامية في العراق والشام (ISIL) على تويتر (Twitter)، ولكن يمكن تطبيق المقاربة على مجموعات مُشبَّكَة أخرى أو منصات تواصل اجتماعي توفّر البيانات لتحليل الشبكات الاجتماعية (SNA).

في هذه المقاربة النموذجية، تم استخدام مناصري الدولة الإسلامية في العراق والشام (ISIL) القائمين من أجل تحديد مناصرين آخرين. وكانت النتيجة مجموعة كبيرة

الجدول رقم 3.1
مقاربات مختارة لتحليل بيانات وسائل التواصل الاجتماعي دعماً لحملات عمليات المعلومات (IO)

المقاربة	التطبيق النموذجي
وصف الشبكات	تحليل وصفي لشبكات المتطرفين باستخدام قوائم العناوين الإلكترونية لأغراض اختبارية والمُختارة يدوياً من أجل استقراء شبكات الدعم وتعقّبها
تحليل فئات العامّة	تحليل لغوي وتحليل للشبكات من أجل الكشف عن مجموعات مُشبَّكَة من المُستَخدِمين الذين ينخرط البعض منهم مع البعض الآخر وتصنيفها ورسم خرائط لها
تحليل الصدى	عمليات قياس لغوي وإحصائي لانتشار رسائل المتطرفين واستيعابها مع الوقت ومن الناحية الجغرافية
تحليل الموقف	تحليل رقمي لتقنيات التجسس وإجراءاته في الرسائل
تحليل الصور الممكنن	الكشف الجغرافي–المكاني ورسم الخرائط للصور المُتبادلة على وسائل التواصل الاجتماعي باستخدام تصنيف الصور الخاصة بالشبكات العصبية العميقة (DNN) وتحديد الموقع الجغرافي/الاستدلال الجغرافي.

[2] قد تكون مقاربات تحليلية مختلفة مفيدة للنظر في المحادثة العامّة **حول** المجموعة على وسائل التواصل الاجتماعي.

إلى حدّ ما من البيانات حول مليون إلى 1.35 مليون مناصر للدولة الإسلامية في العراق والشام نشط على تويتر (Twitter) (برغر [Berger] ومورجان [Morgan]، 2015). شكّل تحديد أفراد الشبكة عمليّة تتألف من ثلاث خطوات، دمجت المقاربات الآلية تحقيقاً لقابلية التوسّع مع إجراءات فحص العينات العشوائي بإشراف بشري تحقيقاً للدقّة.

استخدام الحسابات لأغراض اختباريّة من أجل تحديد أعضاء الشبكة

تمثّلت الخطوة الأولى في العمليّة بتطوير قائمة للعناوين الإلكترونية لأغراض اختبارية مُعالجة يدوياً للأعضاء المتطرّفين المعروفين الذين كانوا نشطين على تويتر (Twitter). إنّها عمليّة تتطلّب عمل كثيف حتّى بالنسبة للخبراء (حوالي أشهرٍ لفريق يتألّف من شخصين). في بحثهم اليدوي للحسابات التي أشارت إلى دعمٍ نشطٍ لمجموعةٍ متطرّفةٍ في نشاط المُستَخدِمين على تويتر، حدّد الباحثون 424 مناصر نشط للدولة الإسلامية في العراق والشام (ISIL) — أو المستوى 0 في نموذج الشبكة.

وتمثّلت الخطوة الثانية باستخدام اتصالات الشبكة المتجانسة من أجل الاستدلال على مناصرين آخرين، انطلاقاً من قائمة العناوين الإلكترونية لأغراض اختبارية. وعلى عكس المقاربات الأخرى التي تستخدم المحتوى من أجل تحديد الانتماء (راجع القسم التالي، "تحليل فئات العامّة: رسم خريطة لأماكن النقاش على وسائل التواصل الاجتماعي")، يُعتبر هنا اتّجاه الاتصال ذا أهميّة. تَخَيَّل مجموعة من مُستَخدِمي تويتر يُعلِّقون على برنامج تلفزيوني مشهور. قد يشمل المُشاركون في هذه التفاعلات أعضاء فريق التمثيل، وطاقم الإنتاج، وممثلين عن الإستديو، وصحافيين، وبالطبع، المعجبين بالبرنامج. إذا حدّدنا أعضاء شبكة البرنامج — النجوم، والمؤلّفين، ومدير البرنامج، وإلى ما هنالك — يمكننا حينئذٍ إجراء تخمينات حول المُستَخدِمين الآخرين الذي يتكلّمون عن البرنامج من خلال تحليل اتجاه اتصالاتهم: قد يكون للنجم عددٌ كبيرٌ جداً من الأتباع (معظمهم من المعجبين) الذين لا يرتبطون مباشرةً بالبرنامج، ولكن من الأرجح أكثر أن يكون الأشخاص الذين **يتبعهم** النَجْم منتمين إلى البرنامج.

وبالتالي، في مثال الشبكة المتطرفة، يقدّم تجاهل الذين يتبعون أعضاء قائمة العناوين الإلكترونية لأغراض اختبارية من المستوى 0 والقيام بدلاً عن ذلك بتحديد الذين **يتبعهم** أعضاء قائمة العناوين الإلكترونية لأغراض اختبارية من المستوى 0 صورةً أكثر دقّةً بشكلٍ محتملٍ عن أعضاء الشبكة المرجّحين (المستوى 1). في هذا المثل، بعد إجراء مسحٍ من أجل إزالة البرمجيات الروبوتية المشتبه بها والبريد المتطفّل، حدّدت هذه المجموعة التي تتألف من خطوة واحدة في الشبكة عدد المُستَخدِمين بحوالي 43,000 مُستَخدِم. ولكن ليس بالطبع الأشخاص جميعهم الذين يتبعهم الأعضاء من المتسوى صفر مناصرين على تويتر للدولة الإسلامية في العراق والشام؛ تدعو الحاجة إلى إجراء اختيارٍ إضافي.

استخدام تشكيل الزُمر (العصابات) والتركيز داخل الشبكة من أجل تحسين تحديد عضوية الشبكة

تمثّلت خطوة ثالثة في تحديد أعضاء الشبكة الذين يدعمون الدولة الإسلامية في العراق والشام (ISIL) بشكلٍ نشطٍ بفرز المُستَخدِمين المتبقين في مجموعة البيانات والبالغ عددهم 43,000 مُستَخدِم بحسب انخراطهم العلني مع الدولة الإسلامية في العراق والشام على تويتر (Twitter)، بالإضافة إلى درجة تشكيلهم للزُمر (العصابات) وتركيزهم داخل الشبكة. في تحليل الشبكات، يتم تعريف هذين المفهومين على الشكل التالي:

- **الزُمر (العصابات)** هي هيكليات فرعية ضمن شبكة حيث تتصّل كل عقدة بعقدة أخرى. تَخَيَّل شبكة كبيرة من مناصري نيو إنجلاند باتريوتس (New England Patriots). ضمن هيكلية تلك الشبكة، قد تَجِد عدداً من الزُمر (العصابات) الصغيرة — مجموعات يعرف فيها الجميع البعض منهم البعض الآخر. قد يكونون مجموعة ضيّقة من الأصدقاء من حيّ في بوسطن، أو ربّما لم يلتقوا يوماً وجهاً لوجه، وإنّما يعرف البعض منهم البعض الآخر من خلال تفاعلاتهم على الإنترنت. الأمر الذي يهم هو درجة تشكيل الحُزم (العصابات)، ما يساعد على تحديد العضوية في الشبكة.
- **التركيز داخل الشبكة** يشير إلى الميل إلى إجراء اتصالات داخل الشبكة أكثر من الاتصالات خارج الشبكة (التفاعلات مع مُستَخدِمين من خارج مجموعة). في مثلنا حول كرة القدم، حتّى المشجّعين العاديين لنيو إنجلاند باتريوتس (New England Patriots) قد يكون لهم اتصالات قليلة داخل الشبكة، ولكن في حال انحراف نسبة أحدهم من حيث الاتصالات بالشبكة — في حال توجيه مُستَخدِم إلى الداخل في الشبكة — يشير ذلك إلى قوّة العضوية.

أثبت فرز الحسابات من المستوى 1 والبالغ عددها 43,000 حساب باستخدام هذه المقاييس مُجتمعة أنّه أكثر دقّة بكثير من استخدام مقياسٍ واحدٍ لتحديد المناصرين. لدى إجراء فحصٍ سريعٍ من قِبَل محلّل بشري، بَيَّنَت هذه المقاربة دقّة عاليةٍ جداً (93 في المئة) للحسابات الـ20,000 الأولى في مجموعة البيانات، ولكن سرعان ما تراجع هذا الرقم إلى دقّة بنسبة 48 في المئة تتجاوز الحسابات الـ30,000 الأولى. ولذلك، في هذا المثل، كان من الممكن بالنسبة للباحثين وصف ديموغرافيات شبكة كبيرة (20,000 مُستخدِم) من مناصري الدولة الإسلامية في العراق والشام النشطين ونشاطها، مع مستوى عالٍ من الثقة بأنّ مجموعة البيانات كانت دقيقة.[3]

[3] في هذه الحالة، تكون تحليلات البيانات الأوسع بخطوات n (خطوات تدريجية) ممكنة — على سبيل المثال،

تحليل فئات العامّة: رسم خريطة لأماكن النقاش على وسائل التواصل الاجتماعي

بالنسبة لما يتجاوز وصف الشبكات الاجتماعيّة لمجموعةٍ متطرّفةٍ مثل الدولة الإسلامية في العراق والشام (ISIL)، يمكن استخدام الجَمْع بين تحليل الشبكات الاجتماعية (SNA) والتحليل اللغوي من أجل تمييز الصراع الأيديولوجي حول الدولة الإسلامية في العراق والشام الجاري على وسائل التواصل الاجتماعي (بودين–بارون [Bodine–Baron]، هيلموس وآخرون [.Helmus et al]، 2016).[4] تستخدم هذه المقاربة خوارزمية كاشفة للمجموعات من أجل تحديد المجموعات المتورّطة والتحليل اللغوي من أجل تمييز هذه المجموعات. وتُعتبر هذه المقاربة طريقةً للتجسيد المرئي ليس لِمَن يتكلّم مع مَن فحسب، وإنّما أيضاً للأمور التي يتكلّمون عنها (ويهتمون بها). تمثّلت النتيجة بخريطة خاصة بوسائل التواصل الاجتماعي لأماكن النقاش حول الدولة الإسلامية في العراق والشام (بودين–بارون [Bodine–Baron]، هيلموس وآخرون [.Helmus et al]، 2016). ويُبيّن الشكل رقم 3.1 خريطة المجموعات الجامعة من المستوى الأوّل التي تمّ اكتشافها في تلك الدراسة، بالإضافة إلى كثافة الاتصالات فيما بينها واتجاهها.

تم تصميم الشكل رقم 3.1 باعتماد عمليّة تتألف من خطوتين. أظهر الكشف عن المجموعات هيكلية الشبكة وميّز التحليل اللغوي للمحتوى من كل مجموعة مجموعات المُستَخدِمين — وبالتحديد، من كانوا ديموغرافياً وما هي الأمور التي يهتمّون بها.

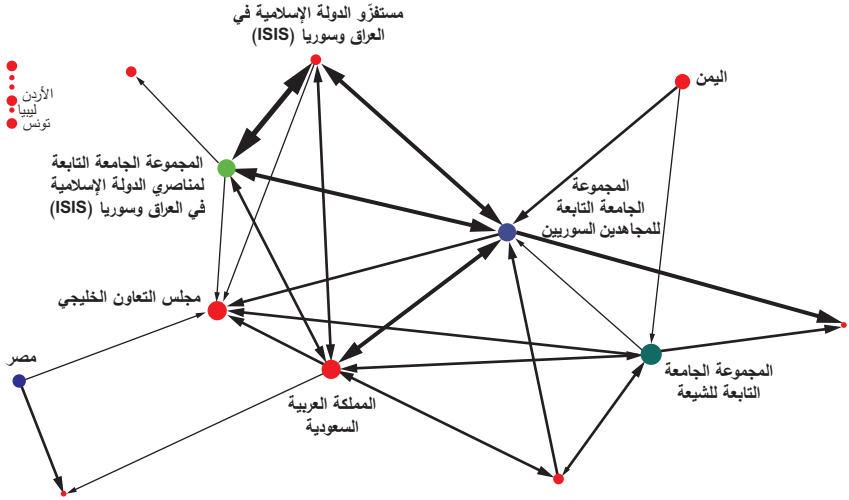
الكشف عن المجموعات

تتمثّل الخطوة الأولى في هذه المقاربة بجمع بيانات وسائل التواصل الاجتماعي حول قضية أو كيان ذي أهميّة — في هذه الحالة، أكثر من 23 مليون تغريدة من أكثر من 770,000 مناصر وخصم للدولة الإسلامية في العراق والشام (ISIL) على تويتر (Twitter) (بودين–بارون [Bodine–Baron]، هيلموس وآخرون [.Helmus et al]، 2016). يقترح الخبراء المتخصّصون في المجال مصطلحات بحث ذات صلة من أجل تحديد المناصرين والخصوم المُرجّحين للدولة الإسلامية في العراق والشام: متغيرات التعابير ودالّة الهاش لكلّ من **داعش** *(Daesh)* و**الخلافة الإسلامية** *(Islamic Caliphate)* باللغة العربية. يمكن بعدئذٍ التحقّق آلياً من الحسّ البديهي للخبراء المتخصّصين في المجال من خلال القراءة الآليّة — عَبْر تطبيق تقنيّات التحليل

التقدّم خطوة واحدة إضافية بعد مُستَخدِمي المستوى 1 من أجل النظر في المُستَخدِمين الذين يتبعونهم ومن ثمّ استخدام أساليب قابلة للتوسّع (مثلاً، التعلّم الآلي) من أجل اختيار الشبكة الأكبر من المناصرين النشطين. راجع برغر (Berger) ومورجان (Morgan) (2015)، للمزيد من التفاصيل حول الموضوع.

[4] يبيّن نطاق هذه الدراسة سبب اعتبار تحليلات بيانات الحاسوب أساسيّة لجهود عمليات المعلومات (IO) وجمع بيانات وسائل التواصل الاجتماعي بشكلٍ أكثر عموماً: أكثر من 23 مليون تغريدة من 771,371 حساب مُستَخدِم.

الشكل رقم 3.1
المجموعات الجامعة المؤيدة والمعادية للدولة الإسلامية في العراق والشام (ISIL) على تويتر (Twitter)



المصدر: بودين–بارون (Bodine–Baron)، هيلموس وآخرون [Helmus et al.]، 2016، ص. 23، الشكل رقم 4.2 تحليل مؤسسة RAND، بيانات تويتر (Twitter) منذ يوليو/تموز 2014 وحتى مايو/أيار 2015.

ملاحظة: تشير سماكة السهم إلى الاتصالات بين المجموعات الجامعة التي تكون أدنى أو أعلى كثافةً بالنسبة لحجم المجموعة. حجم العقدة ممثل لحجم المجموعة. تشير العُقد الحمراء إلى عضوية المجموعة الجامعة السنيّة. نظراً للقيود على الموارد، لم يكن من الممكن دراسة كل المجموعات بواسطة التحليل اللغوي؛ المجموعات التي لم يتم استكشافها تظهر بدون تسميات. MC = المجموعة الجامعة (Metacommunities).

RAND *RR1742-3.1*

اللغوي على البيانات التي تمّ جمعها لرؤية ما إذا توصّل التمييز بين المجموعات التي استخدمت **داعش** مقابل تلك التي استخدمت **الخلافة الإسلامية** إلى تحديد الخصوم والمناصرين بدقّة، على التوالي (وهو أمر يتم وصفه بتفاصيل أكبر في القسم التالي). في هذه الحالة، بيّن اختبار السمة المفتاحيّة أنّ المجموعات التي تستخدم **داعش** بالفعل استخدمت أيضاً مصطلحات تحقيريّة للدولة الإسلامية في العراق والشام (مثلاً، **الخوارج**، إشارةً إلى الخصوم القدامى للاتجاه السائد للإسلام) ومصطلحات تدلّ على الاحترام للدول العربيّة والغربيين (مثلاً، **الائتلاف الدولي**).[5] استخدمت المجموعات التي تشير

[5] ينطوي اختبار السمة المفتاحيّة على اختبار تواتر الكلمات التي تم العثور عليها مقابل الكلمات المتوقّعة للكشف إحصائياً عن الوجود المفرط أو الوجود القليل. يمكن قياس التواتر المتوقّع مقابل معيار عام (مثلاً، مدوّنة أحاديّة اللغة، مثل المدوّنة العربية المفتوحة المصدر [Open Source Arabic Corpora]) أو معيار محدّد (مثلاً، مجموعة واسعة من المحادثات اليومية العامّة على وسائل التواصل الاجتماعي). للاطّلاع على خلفيّة إضافية حول هذه التقنيّات، راجع سكوت (Scott) (2011).

إلى **الخلافة** مصطلحات تدلّ على الاحترام للدولة الإسلامية في العراق والشام (مثلاً، **أسود الدولة الإسلامية**) ومصطلحات مسيئة للدول العربية (بما فيها **المرتدّون**) وللغربيين (**الصليبيون**). شكّلت هذه العملية نوعاً من إجراءات التحقق من الصحّة، مشيرةً إلى أنّ مصطلحات البحث هذه كانت وسائل فعّالة للتفريق: حدّد بفعالية استخدام مصطلح واحد مقابل مصطلحاً آخر موقف مُستَخدِم إزاء الدولة الإسلامية في العراق والشام.

ما إن تمّ تطبيق خوارزمية كاشفة للمجموعات على البيانات، يتيح هذا التحقّق اللغوي اتخاذ خطوة تالية مهمّة. تُعتبر بيانات تويتر (والبيانات من منصّات مماثلة، مثل سينا ويبو [Sina Weibo]) قابلة للتحويل إلى تحليل الشبكات الاجتماعية (SNA) لأنّ الإجابات والتنويهات والتغريدات المُعاد إرسالها تحدد التفاعلات على الشبكة. من خلال رسم خريطة لهذه التفاعلات جميعها وتحليلها، يمكن لخوارزمية كاشفة للمجموعات أن تُجمِّع المُستَخدِمين بسرعةٍ ضمن هيكليات مترابطة، ولكنّها لا تستطيع تسميتهم أو تمييزهم. تجد الخوارزمية ببساطة المجموعة 1، والمجموعة 2، وإلى ما هنالك. ولكنّ وسيلة التفريق **داعش** مقابل **الخلافة** قد طبعت كل مجموعة باعتبارها مؤيدة للدولة الإسلامية في العراق والشام، أو معادية للدولة الإسلامية في العراق والشام، أو مختلطة من حيث دعمها للمجموعة.

تمييز المجموعات

في حين يتم استخدام تحليل الشبكات الاجتماعية (SNA) لتحليل المجموعات وتفاعلاتها البعض منها مع البعض الآخر — وبيّنت وسيلة التفريق **داعش/الخلافة** المواقف المؤيدة وتلك المعادية — من منظور عمليات المعلومات (IO)، لا تزال الخريطة فارغة ومن دون علامات. بدون فهم الخصائص والمخاوف الخاصة بأطراف النقاش حول الدولة الإسلامية في العراق والشام (ISIL)، ما من طريقة معقولة للتأثير على المحادثة.

وتتمثّل مشكلةٌ بكون مجموعة التغريدات كبيرةً جداً بالنسبة للتحليل البشري. وبالنسبة لما يتجاوز قابلية التوسّع، قد تبقى الموثوقية والتحيّز البشريين يشكلان مشكلة. يتطلّب تمييز هذه المجموعة بشكلٍ قابل للتوسّع وموثوق تحليلاً آلياً لمحتوى تغريدات المجموعات التي تم الكشف عنها. ويتمثّل حلٌّ بالأساليب التحليلية المرتكزة إلى الآلة من عِلْم لغة المدوّنة الحاسوبية (التحليل اللغوي). يعتمد التحليل اللغوي على اختبارات إحصائية لتواتر الكلمات أو للمسافة بين الكلمات، ما يكشف عن هيكلية البيانات النصيّة. في هذه الحالة، تم تطبيق أسلوبين على البيانات النصيّة: اختبار **الكلمات المفتاحية** و**العبارات المترافقة**. تحدّد الكلمات المفتاحية الكلمات الموجودة بشكلٍ مفرط إحصائياً في مجموعة بيانات نصيّة وتُبيّن الموضوع الأولّي للنصّ الذي تم جمعه (سكوت [Scott]، 1996، 2001). لأنّه يتم وزن الكلمات المفتاحيّة بمدى اعتبارها غير اعتياديّة إحصائياً، يقترن اختبار

الكلمات المفتاحيّة بقوّة تفريق أكبر للإشارات الأضعف. على عكس الكلمات المفتاحية، تُعتبر العبارات المترافقة جليّةً إحصائياً لأنها تشير إلى الكلمات المترافقة (بايكر وآخرون [Baker et al.]، 2008)، وهي غالباً ما تلتقط أفكار مستخلصة.[6]

تحديد فئات العامّة واستراتيجيات التأثير المحتملة

يتيح الكشف الممكنن للكلمات المفتاحية المهمّة استراتيجياً والعبارات المترافقة المرتبطة بها بقوّة تمييز المجموعات التي تمّ الكشف عنها باعتبارها **فئات من العامّة:** أفكار مستخلصة لأشخاص لديهم مصلحة تحقيق التأييد، باستخدام لغة مشتركة من أجل معالجة مشكلة مشتركة. ولاستخدام مثلٍ مألوفٍ بالنسبة للجماهير الأمريكية، أُنْظُر في قضية مثل السيطرة على الأسلحة. فمن جهة، تُعتبر الرابطة الوطنية لحملة البنادق في أمريكا (National Rifle Association) مثلاً من العالم الحقيقي حول منظّمة معنيّة بالتأييد، ولكنّ العامّة التي تستخدم لغة مشتركة وتتشاطر هدف واحد هو شرعنة الملكيّة الخاصّة للأسلحة هي استخلاص أكبر بكثير. وتُعتبر العامّة المعارضة التي تسعى إلى الحدّ من ملكية الأسلحة أكبر أيضاً من أي جماعة ضغط رسميّة: إنّها مجموعة الأشخاص الذين يهتمّون بقضية ويستخدمون خطاباً مشتركاً للتأثير على النقاش.

بالعودة إلى مثلنا الأصلي حول تمييز مناصري الدولة الإسلامية في العراق والشام (ISIL) على تويتر (Twitter)، كشف تحليل الشبكات الاجتماعية (SNA) عن أربع مجموعات جامعة كبيرة، التي يمكن أن يميّزها التحليل اللغوي بوصفها فئات جامعة من العامّة (بودين–بارون [Bodine–Baron]، هيلموس وآخرون [Helmus et al.]، 2016). طبعت مجموعةً كلماتٌ مفتاحيةٌ وعباراتٌ مترافقةٌ تعكس المخاوف السعودية (بما في ذلك القومية السعودية)، وكلماتٌ علمانيّة أو دينيةٌ سلبيةٌ حول الدولة الإسلامية في العراق والشام (الإرهابيون، الجرائم والذنب، والمحرمون، **والفتنة**)، وبعض الكلمات الإيجابية مع دلالات دينية (التسبيح، التكبير، الحقيقة، الحب). **وتتمثّل هنا نقطة رئيسيّة يتوجّب استخلاصها بأنّه بدلاً من فريق من المحلّلين يقرأ ملايين التغريدات، يمكن لمحلّلٍ واحدٍ يستخدم برمجيات التحليل اللغوي أن يحدّد مئات الكلمات والتعابير غير الاعتيادية استراتيجياً أو ما يقارب ذلك من أجل تمييز مجموعة بوصفها فئة من العامّة.** كانت الفئات الأربعة الكبيرة من العامّة التي تمّ استكشافها في هذا المثل على الشكل التالي:

- الخصوم السنّة للدولة الإسلامية في العراق والشام (ISIL) (بعض المناصرين)
- الخصوم الشيعة للدولة الإسلامية في العراق والشام (ISIL)

[6] مثلاً، أسماء الأماكن ("مدينة نيويورك")، والكيانات ("الرئيس أوباما")، والمفاهيم المستخلصة ("السيطرة على الأسلحة").

- مناصرو الدولة الإسلامية في العراق والشام (ISIL)
- المجاهدون السوريون (مع موقف مختلط إزاء الدولة الإسلامية في العراق والشام).

يتيح تحليل الشبكات الاجتماعيّة والتحليل اللغوي معاً تحليلاً أكثر تفصيلاً حتّى، موفّراً قاعدةً تجريبيةً للرسائل المعقولة من أجل التأثير على فئات محددة من العامة. يبيّن الجدول رقم 3.2 فئات العامّة الفرديّة (المُنظّمة بشكلٍ أساسيّ حول الهويات والمخاوف الوطنية) والمُحدّدة ضمن العامّة الجامعة السنيّة، بالإضافة إلى المخاوف الخاصة بكلّ واحدة منها والمواضيع التي تعتبر ذات أهمية بالنسبة لها.

وتوفّر مواضيع كل فئة من العامّة ومخاوفها قاعدة تجريبية لاستراتيجيات الرسائل المعقولة والتأثير المستهدف الموجّه نحو أعضاء هذه الفئات من العامّة. هنا، نشدّد على قابلية توسّع هذه المقاربة وقيمتها الاستقرائية على حدّ سواء. كان هذا عمل محلّل وحيد على مدى أيّام، وليس فريق يستغرق أشهراً لقراءة مئات آلاف التغريدات. ولأنّ التحليل يعتمد بشكلٍ حصريّ على بيانات وسائل التواصل الاجتماعي التي يولّدها المُستَخدِم، ثمّة فرصة ضئيلة للتوقّع — توقّع الرسائل التي تعكس الافتراضات والأولويّات الثقافية الأمريكية — ويمكن إجراؤه على مستوى تفصيلي إلى حدّ ما.

الجدول رقم 3.2
فئات العامة السنيّة في تحليل معارضة/دعم الدولة الإسلامية في العراق والشام (ISIL) على تويتر (Twitter)

العامّة السنيّة	المواضيع والمخاوف
المملكة العربية السعودية	التهديد لدعم الدولة الإسلامية في العراق والشام (ISIL) وتوسّعها داخل المملكة العربية السعودية؛ التهديد للإسلام الذي يطرحه التشيّع الإيراني؛ القوميّة العلمانيّة؛ والمجتمع الدوليّ
مصر	القوميّة المصريّة؛ معارضة الدولة الإسلامية في العراق والشام (ISIL)؛ الارتياب من تنظيم الإخوان المسلمين؛ الاستياء من السياسات الأمريكية
الأردن	القوميّة؛ الغضب من إحراق الدولة الإسلامية في العراق والشام (ISIL) للطيّار الأردني مُعاذ الكساسبة، دعم الحملة الجويّة للائتلاف الدوليّ
ليبيا	القومية الليبيّة؛ معارضة الدولة الإسلامية في العراق والشام (ISIL)؛ الارتياب من السياسيين الليبيين والمقاتلين، والغرب
اليمن	دعم الدولة الإسلامية في العراق والشام (ISIL)؛ انتقاد تدخّل المملكة العربية السعوديّة

المصدر: بودين–بارون (Bodine–Baron)، هيلموس وآخرون [Helmus et al.]، 2016، ص. 31، الجدول رقم 5.1؛ تحليل مؤسسة RAND لبيانات تويتر (Twitter) منذ يوليو/تموز 2014 وحتّى مايو/أيار 2015.

تحليل الصدى: تعقّب انتشار الرسائل على وسائل التواصل الاجتماعي

يفصّل هذا القسم أسلوباً لتعقّب استيعاب رسائل مجموعة مع الوقت على مستوى جغرافي تفصيلي إلى حدّ ما. تعقّبت دراسة إثبات المفهوم الوارد وصفها هنا استيعاب اللغة الخاصّة بالنظرة العالمية التي يعتمدها أعضاء الدولة الإسلامية في العراق والشام (ISIL) والإخوان المسلمين (Muslim Britherhood) في مصر عام 2014 (مارسيلينو وآخرون [Marcelino et al.]، 2016). على الرغم من ذلك، يقترن هذا الأسلوب بقدرةٍ واسعةٍ بوصفه مقياساً للفعالية، بما في ذلك بالنسبة لجهود الرسائل الوديّة.

تتمثّل القاعدة لهذا الأسلوب بالعلاقة الوثيقة بين اللغة والنظرة العالمية، حيث تعكس اللغة النظرة العالمية وتتشكّل في المقابل أيضاً النظرة العالمية بفعل استخدام اللغة. يمكننا أن نرى هذه العلاقة بوضوح كبير في اللغة حول القضايا المتنازع عليها. لا يعكس الاستخدام المتّسق لكلمات في خطاب حول قضية محدّدة الأيديولوجية فحسب؛ يساعد استخدامها أيضاً في تداول الأيديولوجية ونشرها من خلال رسم إطارٍ للقضايا والأحداث في العالم. وبما أنّنا نستطيع تصميم خطاب عامّة من الناحية الكميّة، يمكننا تعقّب استيعاب نظرة عالمية كما يتم التعبير عنها من خلال اللغة.

بناء نموذج لغوي

تتمثّل الخطوة الأولى في هذا الأسلوب ببناء نموذجٍ لغوي موزون لحديث فئة من العامة. في هذا المثل، يتعلّق الأمر بمجموعة متطرّفة، ولكن يمكن أن تكون بهذه البساطة قيادة مقاتلين ورسائلها الإقليمية. في هذا المَثَل لإثبات المفهوم، جمع المحلّلون بيانات حول حديث عامّة من الدولة الإسلامية في العراق والشام (ISIL) والإخوان المسلمين على حدّ سواء (حوالي 30,000 كلمة لكل واحدة) ثمّ اختبروا مجموعة البيانات بحثاً عن الكلمات المفتاحية والعبارات المترافقة على حد سواء. أنتَجَ ذلك نموذجاً لغوياً لكل مجموعة يضمّ حوالي 100 كلمة مفتاحية مهمّة إحصائياً و20 عبارة مترافقة تتألّف من كلمتين. وللمساعدة في تشكيل مفهومٍ لما نعني **بنموذج لغوي موزون**، يقدّم الجدول رقم 3.3 بعض الكلمات المفتاحية النموذجية، والدرجات المحرزة في اختبار الرجحان اللوغاريثمي، والترجمة لكل كلمة.

في هذا الاختبار المحدد، تُعتبر الدرجات المحرزة في اختبار الرجحان اللوغاريثمي التي تفوق 11 مهمّة. في الجدول رقم 3.3، تشير الدرجات المحرزة التي تتألف من رقمين لكلمات مثل **العراق** أو **الشام** إلى أنّها موجودة بشكلٍ مفرطٍ كثيراً وقابلة للكشف، في حين تُعتبر الدرجات المحرزة في المئات (مثلاً، **رافضي**) إشاراتٍ دلاليّة قويّة جداً لموضوع النصّ الأوّلي. وتبيّن الدرجات المحرزة التي تفوق 1,000 حديثاً متخصّصاً إلى حد كبير وبالتالي، إشارةً مميزةً: في حين قد لا تكون كلمات مثل **الصفوي** مواضيع من المستوى الأوّل والتي قد يفكّر فيها محلّل كيفي (وصفي) لدى محاولة فهم رسالة الدولة الإسلامية

الجدول رقم 3.3
كلمات مفتاحية نموذجية للدولة الإسلامية في العراق والشام (ISIL) والإخوان المسلمين، والترتيب في اختبار الرجحان اللوغاريثمي

الدولة الإسلامية في العراق والشام (ISIL)			الإخوان المسلمون		
الكلمة المفتاحية	الرجحان اللوغاريثمي (LL)	الترجمة	الكلمة المفتاحية	الرجحان اللوغاريثمي (LL)	الترجمة
الصفوي	2,163	The Safavid	الإخوان	2,882	The Brotherhood
الدولة_الإسلامية	643	The Islamic State#	الانقلاب	1,631	The coup
الخلافة	640	The caliphate	الشعب	914	The people
الفلوجة	427	Fallujah	الجماعة	434	The association
البيشمركة	360	The Peshmerga	المصري	395	The Egyptian
الرافضي	271	The Rafidhi	مصر	332	Egypt
الدولة	259	The state	الرييس	329	The president
الإسلامية	585	The Islamic	الثوار	319	The revolutionaries
القاعدة	123	Al Qaeda	جماعة	266	The group
العراق	78	Iraq	الانقلابيين	265	The coup supporters
الشام	62	Sham	الإرهاب	257	The terrorism

المصدر: مارسيلينو وآخرون [Marcelino et al.]، 2016، ص. 45، الجدول رقم 1.

ملاحظة: بالنسبة لاختبار الرجحان اللوغاريثمي، تساوي القيمة الحرجة 10.83 (0.01 في المئة؛ $p<0.001$). في هذا المثل، بلغ الحدّ الأدنى من التواتر 20. لتفسير الدرجات المحرزة في اختبار الرجحان اللوغاريثمي (LL) في هذا الجدول، نشير إلى أنّ درجة محرزة في اختبار الرجحان اللوغاريثمي تفوق 11 (LL>11) هي مهمّة إحصائياً، وتشير درجة تتراوح بين 11 و1,000 إلى مستويات عالية من السمة المفتاحية (حديث محدد جداً)، وتشير الدرجات التي تفوق 1,000 إلى كلمات مفتاحية تحدد الخطابات المتخصصة جداً.

في العراق والشام (ISIL)، من منظور تجريبي لمحاولة الكشف عن إشارات ضعيفة (مثلاً، آثار التأثير)، يشكّل هذا التواتر العالي بشكلٍ غير متوقّع جزءاً تحليلياً قوياً ملفتاً للانتباه.

مرفقة بتوقيع — نموذج موزون كمّي لكيفية تحادث هذه المجموعات السلفيّة، تتمثّل الخطوة الثانية بقياس درجة التوافق بين ذلك النموذج والحديث من عامّة الجمهور: هل تكتسب هذه المجموعات أو تخسر الأرضيّة في نشر رسائلها؟

التطابقات الإقليمية للحديث على وسائل التواصل الاجتماعي والرسائل المتطرّفة

بالنظر إلى نموذج لغوي لحديث مجموعة متطرّفة، يمكن رؤية درجة تطابق مُستخدِمي وسائل التواصل الاجتماعي في المجموعة العامة مع ذلك الحديث — تطابق كمّي لحصّة السوق الاستطراديّة لمجموعة. تَخَيَّل رصد حديث على وسائل التواصل الاجتماعي في شمال شرق الولايات المتحدة حول موضوع ملكية الأسلحة الخاصّة. على أساس ربع سنوي، زاد الأفراد هناك استخدامهم لمصطلحات مثل **إطلاق النار الجماعي**، و**أعمال القتل الطائشة** و**البريء**، وحصلت أحاديث أقلّ شملت كلمات مثل **الملكية المسؤولة** و**حقوق التعديل الثاني (لدستور الولايات المتحدة)** و**المجرمون**. قد يشكّل ذلك أسساً قويةً وتجريبيةً من أجل الجدل بأنّ طرف واحد كان يحرز المكاسب في الرأي العام، أقلّه من حيث رسم إطار للحجة على أنها تدور حول خطر الأسلحة بدلاً من قضية مرتبطة بالحريات المدنية.[7] إن العمليّة العامّة هي على الشكل التالي:

- **جمع بيانات وسائل التواصل الاجتماعي من مجموعةٍ جغرافيةٍ هادفة.** في مثلنا الأوّلي، كان المصدر بيانات تويتر (Twitter) من أنحاء مصر عام 2014، مع استدلال جغرافي إلى أربع مناطق: سيناء، الإسكندرية والساحل، صعيد مصر، والقاهرة ودلتا النيل. في هذا المثل، أدّى الاستدلال الجغرافي مُستخدِماً أسماء المدن والمحافظات على حدّ سواء في حقل موقع المُستَخدِم إلى مضاعفة حجم البيانات التي تم التقاطها، ولكن، لدى فحصها بالمقارنة مع البيانات التي تحمل وسماً جغرافياً، كان له حدّ ثقة أدنى لدقة تساوي 80 في المئة.
- **تحديد درجة تغذيات مُستَخدِمي تويتر (Twitter) للتطابقات الإحصائية مع النماذج اللغوية.** يمكن تحديد درجة تغذية كل مُستخدِم على تويتر (Twitter) انطلاقاً من مدى تطابقها عن كثب مع نموذج لغوي (مثلاً، الدولة الإسلامية في العراق والشام [ISIL] أو الإخوان المسلمون):
  – ينطوي ذلك على جمع الدرجات المحرزة في اختبار الرجحان للكلمات المفتاحية

[7] نلاحظ أنّ هذه المقاربة لا تسمح لنا بالإجابة عن سبب حصول هذا التغيّر، وإنّما بملاحظة أنّه حصل فحسب. قد تتطلّب الرؤية السببية مقاربات أخرى.

والتعابير المترافقة كلها التي تظهر في تغريدات كلّ مُستَخدِم ومن ثم احتساب المجموع المتوقّع باحتمالٍ عشوائي، بالنظر إلى العدد الإجمالي للكلمات التي تظهر في تغريدات المُستَخدِم والتواتر/الدرجة المتوسطة للكلمات المفتاحية والعبارات المترافقة بين التغريدات جميعها.

– تُعتبر الدرجات المحرزة الناتجة عن ذلك مقياساً لمدى احتمال أن تكون هذه التطابقات مجرّد احتمال عشوائي:

- **عالٍ** يعني أنّ حساباً يستخدم أكثر من 500 في المئة من اللغة النموذجية الإضافية (الدولة الإسلامية في العراق والشام [ISIL] أو الإخوان المسلمون) بالمقارنة مع ما هو متوقّع من الاحتمال العشوائي.
- **متوسّط** يعني أن حساباً يستخدم أكثر من 300 في المئة من اللغة النموذجية الإضافية بالمقارنة مع ما هو متوقّع من الاحتمال العشوائي وإنّما أقلّ من 500 في المئة.
- **منخفض** يعني أكثر من 50 في المئة من اللغة النموذجية الإضافية وإنّما أقلّ من 300 في المئة من الاحتمال العشوائي.
- **لا تطابق** يعني أنّ لغة حساب تعكس مستويات الاحتمال العشوائي.

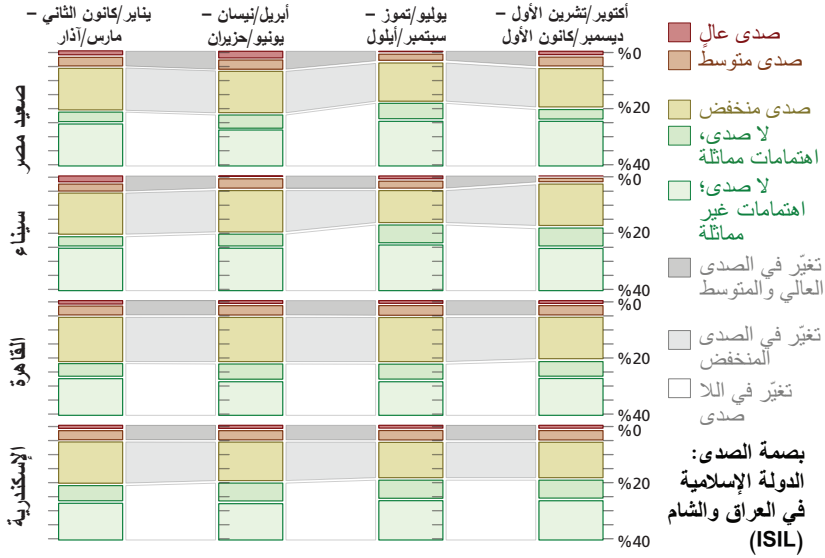
- **رسم خريطة للتغيّر مع الوقت**. يمكن تجميع التطابقات العالية، والمتوسطة، والمنخفضة والـلا تطابقات الكميّة على مستوى المُستَخدِم على المستوى الإقليمي: مقياس للمستوى الحالي من نشر رسائل مجموعة. بالمقارنة على أساس ربع سنوي، إنها طريقة من أجل قياس الفعالية مع الوقت وأيضاً وبشكلٍ محتمل من أجل فرز الجهود الأخرى على حد سواء.

في الحالة النموذجية، كان للدولة الإسلامية في العراق والشام (ISIL) والإخوان المسلمين على امتداد عام 2014 تطابقٌ منخفضٌ في منطقتي الإسكندرية والقاهرة — وتلك أخبار جيّدة من منظور أمريكي. ولكن في سيناء وصعيد مصر على حدّ سواء، حققت الدولة الإسلامية في العراق والشام مكاسب بشكلٍ ملحوظ من حيث عدد تطابقات الصدى العالية والمتوسطة، في حين خسر الإخوان المسلمون كميّة مماثلة. اكتسبت الدولة الإسلامية في العراق والشام بشكلٍ أساسي حصّة سوق في هاتين المنطقتين — وتلك أخبار سيئة من منظور أمريكي. ويبيّن الشكلان رقم 3.2 و3.3 هذا التغيّر في حصّة السوق.

تحليل الموقف: الكشف عن استراتيجيات الرسائل على وسائل التواصل الاجتماعي

لماذا يُعتبر بعض استراتيجيات رسائل المتطرّفين ناجحاً في حين يفشل البعض الآخر؟

الشكل رقم 3.2
الصدى اللغوي للدولة الإسلامية في العراق والشام (ISIL) في مصر، 2014



المصدر: مارسيلينو وآخرون [Marcellino et al.]، 2016، ص. 47، الجدول رقم 2.

RAND *RR1742-3.2*

هل تستطيع وزارة الدفاع الأمريكية (DoD) تحليل الرسائل الناجحة من أجل اكتساب رؤية من حيث تقنيات التجسس وإجراءاته حول عمليات المعلومات (IO)، وفهم سبب كون بعض رسائل الخصوم فعّالاً بشكلٍ خاص فهماً أفضل، وتعلّم كيفية زيادة فعالية رسائلها الخاصّة، بغضّ النظر عن وسائل الإعلام المُستَخدَمة من أجل تعميمها؟ ينظر تحليل الموقف في الرسائل على وسائل التواصل الاجتماعي من أجل الكشف عن التفاصيل اللغوية الخاصة بتلك الرسائل بهدف فهم كيفية عملها بشكلٍ أفضل. يُشبه ذلك تحليل المشاعر، ولكنّه أكثر تفصيلاً وتطوراً. في حين استخدمت المقاربات التي جرت مناقشتها سابقاً في هذا الفصل التحليل اللغوي (اختبارات إحصائيّة على مستوى أعداد الكلمات وتواترها)، يستخدم هذا الأسلوب اختبارات الأعداد والتواتر الإحصائية على مستوى فئات الكلمات. ونعني بـ**فئات الكلمات** مثلاً الحديث عن المستقبل أو الماضي، أو العواطف (مثلاً، الغضب، الحزن، الخوف، الإيجابية)، أو اليقين، أو القِيَم أو العلاقات الاجتماعية. يعتبر تجميع فئات الكلمات في حُجَج فنّاً هادفاً ويُفصح عن إشارةٍ قابلة للكشف. على سبيل المثال، يمكن أن يكون الحديث عن المستقبل والأمل استراتيجيةً لتحفيز الناس، تختلف جدّاً عن خيار جمع الحديث حول الماضي والأخطاء

الشكل رقم 3.3
الصدى اللغوي للإخوان المسلمين في مصر، 2014

المصدر: مارسيلينو وآخرون [Marcellino et al.]، 2016، ص. 49، الجدول رقم 3.

RAND *RR1742-3.3*

التاريخيّة. من خلال الاختبارات الإحصائية حول التواتر، وتوزيع فئات الكلمات ومتغيّراتها المُشاركة، يمكن أن يكشف التحليل المرتكز إلى الحاسوب عن المكونات العاملة من الحُجَج والرسائل على مستوى التفاصيل (مارسيلينو [Marcellino]، 2015).

كتوضيح، تَخَيَّل أنّ رئيس أركان جديد أرسل مذكرة لأعضاء مركز نظاميين ومدنيين. تم تقبُّل المُذكّرة بشكلٍ ضعيفٍ جداً: كان الهدف منها إلهام الأركان للعمل معاً من أجل تصحيح أوجه القصور، ولكن بدلاً عن ذلك، كان لها التأثير العكسي وولّدت كمّاً كبيراً من الغضب تجاه الرئيس الجديد. لدى الاستفسار عن هذا الموضوع، قد يشير الأركان إلى "نبرة" المُذكرة — التي تبدو بعيدة ومتعجرفة. ولكن لماذا، بالتحديد، "تبدو متعجرفة"؟ قد يبيّن فحص الخيارات اللغوية عن كثب أنّ المذكّرة غنيّة بضمائر المتكلّم المفرد وضمائر المخاطَب المفرد وإنّما تفتقر بالكامل إلى ضمائر جماعة المتكلّمين: الضمائر المُستَخدَمة جميعها هي "أنا/ضمير المتكلّم في حالة المفعوليّة" لدى التحدّث عن الحلول، "ضمائر المخاطَب المفرد" لدى التحدّث عن المشاكل، ولم يتم استخدام "نحن/ضمائر جماعة المتكلّمين" البتة للتحدّث عن أي شيء. حتّى وإن لم يكن رئيس الأركان يقصد ذلك، يؤدّي الاستخدام المستمرّ للضمائر بتلك الطريقة إلى نوعٍ من

الموقف المُتَفَوّق تجاه الجمهور. بالنسبة لما يُشبه ملاحظة واحدة، قد يكون التحليل الذي يجري يدوياً من قِبَل محلل خطابات فعالاً وكفؤ. على الرغم من ذلك، بالنسبة للأحجام الضخمة من بيانات وسائل التواصل الاجتماعي، يُطلب إجراء تحليل حسابي.

إيجاد عوامل كامنة في حديث الدولة الإسلامية في العراق والشام (ISIL) على وسائل التواصل الاجتماعي

لاختبار هذه المقاربة، أجرينا تحليلاً توضيحياً لمجموعة من مخرجات وسائل التواصل الاجتماعي من أربع مجموعات متطرّفة: الدولة الإسلامية في العراق والشام (ISIL)، جبهة النصرة (al-Nusrah Front)، تنظيم القاعدة في شبه الجزيرة العربية (al Qaeda in the Arabian Peninsula [AQAP])، وأنصار الشريعة (Ansar al-Sharia).[8] استخدمنا ثلاثة أشهر من مخرجات وسائل التواصل الاجتماعي المُترجَمة من هذه المجموعات في الفصل الرابع من عام 2014.[9] استخدمنا بعدئذٍ أحدث البرمجيات (اعتباراً من 2015) لتحليل الموقف من أجل التوصّل إلى تواتر فئات الكلمات لكلّ مدوّنة، والتي أخضعناها لاختبارات التواتر والتوزيع والمتغيّرات المشاركة الإحصائية من أجل الكشف عن أوجه الاختلاف بين المجموعات والانتظامات الهيكلية في خطاب كلّ مجموعة.

للتوضيح، نَصِفُ بالتفصيل نتيجةً مُستخلصةً واحدةً من هذا التحليل: عندما استخدمنا تحليل العامل الاستكشافي للبحث عن هيكليات الحُجج الكامنة، وجدنا أنّه كان للدولة الإسلامية في العراق والشام وجبهة النصرة ثلاثة عوامل (حجج مُقنعة، شهادة شخصية، وتركيز على مخاوف اجتماعية مشتركة)، في حين كان لمخرجات وسائل التواصل الاجتماعي الخاصة بتنظيم القاعدة في شبه الجزيرة العربية عامل واحد (أدلّة إرشادية للمشاكل التقنية). يكشف تحليل العامل الاستكشافي عن الحالات الكامنة من خلال المتغيرات المُشاركة في مجموعة بيانات عَبْر معالجة الصلة بين مجموعة من المتغيرات كعامل واحد كامن. في التحليل النصي، قد يبدو ذلك حديثاً إيجابياً موجّهاً نحو المستقبل ولغة مُطمئنة مع المتغيّرات المُشاركة جميعها معاً مثل: خطاب "تصبح الأمور أفضل مع تقدّمك بالسنّ" الاعتيادي والمُستَخدَم بانتظام. تحدّد الأمثلة التالية العوامل التي تميّز حديث تنظيم القاعدة في شبه الجزيرة العربية العام على وسائل التواصل الاجتماعي

---

[8] نشير إلى أنّ هذا التحليل أوّلي وقد أُجري بوصفه إثبات للمفهوم بالنسبة للأسلوب. كانت مجموعة البيانات صغيرة نسبياً (ثلاثة أشهر من مخرجات وسائل التواصل الاجتماعي من المجموعات المتطرفة)، واستخدم التحليل الترجمات. في حين يوجد دليل أوّلي على أنّ البرمجيات المُستخدَمة في هذا التحليل تعمل بصورة جيّدة في مجال الترجمة (راجع مثلاً المالكي [Al-Malki] وآخرين، 2012)، نحذّر بشدّة من دقّة النتائج المستخلصة. هدفنا في هذا القسم هو توضيح الأسلوب، وليس استكشاف نتائج مستخلصة محددة من إجراء إرشادي للأسلوب.

[9] استخدم هذا التحليل بيانات من اشتراك تجاري في شركة سايت انتليجنس جروب (SITE Intelligence Group) لرصد الجهاديين وتحليلهم.

عن حديث جبهة النصرة والدولة الإسلامية في العراق والشام.[10]

استراتيجيّة حُجج تنظيم القاعدة في شبه الجزيرة العربية (AQAP)

كان عامل التفريق المهمّ بالنسبة لتنظيم القاعدة في شبه الجزيرة العربية (AQAP) **معلوماتيّ:** تبادل المعرفة التقنيّة والمفاهيميّة والإبلاغ عن الأحداث المهمّة.

ظهر ذلك بالشكل الأكثر قوّة في التعليمات التقنيّة الإرشاديّة التي تتراوح بين الحرب الإلكترونيّة وتجنّب الكشف الحراري. على سبيل المثال،

> يبيّن هذا المشهد مجموعة من المُجاهدين الذين يحاولون الاختباء من كاميرات الطائرات في ممرّ ضيّق، ولكنّ التسجيل الحراريّ يبيّن أجسادهم بوضوح، وبالأخصّ ضمن هذا الارتفاع المنخفض للطائرة. وبالتالي، يبدو أنّ الحلّ هو إخفاء حرارة الجسد عن كاميرات الطائرات. إنّ الطريقة التي تتيح للولايات المتّحدة القيام **بذلك هي** تلك التي تُسمّى العزل الحراري. **إنّ** العزل الحراري مُستَخدَم في عددٍ من الأدوات التي نستخدمها يومياً، مثل قارورات المياه العازلة للحرارة. إنّها تحافظ على حرارة المياه الموجودة بداخلها، لأنّها تحتوي على مادّة عازلة تحول دون تسرّب الحرارة إلى الخارج. وبالإضافة إلى ذلك، يستخدم البرّاد أو ما يسمّى الثلّاجة، وقارورة الشاي العازلة للحرارة أو ما يسمّى وعاء، مفهوم العزل.[11]

كان النمط نفسه واضحاً في الإبلاغ المعلوماتي:

> تُوفّي جندي من الجيش الحوثي المُنقلب [عضو] يوم الخميس الماضي هذا كنتيجةٍ **لتعرّضه** للقنص من قِبَل مُجاهد من أنصار الشريعة في محافظة أبيَن في جنوب اليمن. نقل مراسل أخبار أنصار الشريعة في أبيَن أنّه بتمام الساعة العاشرة صباحاً من يوم الخميس الماضي هذا قَنَص مُجاهد من أنصار الشريعة جندياً في اللواء 39 مُدرّع والذي يتمركز في منطقة المحفد في محافظة أبيَن.[12]

استراتيجيات حُجج الدولة الإسلامية في العراق والشام (ISIL) وجبهة النُصرة

تتقاسم الدولة الإسلامية في العراق والشام (ISIL) وجبهة النُصرة على حدّ سواء ثلاثة حالات كامنة. على عكس مقاربة تنظيم القاعدة في شبه الجزيرة العربية (AQAP)

---

[10] لم يكن لأنصار الشريعة أي عامل قابل للكشف — كان خطاب هذه المجموعة غير متسق وقد افتقر إلى استراتيجيات متكررة ومتماسكة.

[11] ترد المفاهيم بالخطّ المائل، **وحالات التبليغ** بالخطّ العريض في حين يتم وضع خطّ تحت اللغة المحدّدة.

[12] ترد المفاهيم بالخطّ المائل، **وحالات التبليغ** بالخطّ العريض في حين يتم وضع خطّ تحت اللغة المحدّدة.

التقنيّة لتبادل المعلومات، استخدمت الدولة الإسلامية في العراق والشام وجبهة النُصرة استراتيجيات رسائل هادفة في العالم الاجتماعي الثقافي من أجل إقناع جمهوريهما.

التوعية: الوعد بمستقبلٍ أفضل

استخدمت جبهة النُصرة (والدولة الإسلامية في العراق والشام [ISIL]) استراتيجيات توعية مماثلة. وبشكلٍ غير متوقّع ربّما، لم تشمل استراتيجية الحُجج المُهيمنة الخاصّة بهما خطاباً سلبياً أو مُفْعَم بالكراهية، وإنّما، بدلاً من ذلك، حديثاً مكثّفاً وموجهاً نحو المستقبل والذي ركّز على القِيَم والعلاقات الإيجابية.[13] على سبيل المثال،

> إنّ مَن يريد دعم الله **عزّ** وجلّ، دعه إذاً يعلن ولاءه لهذا الخليفة. وإنّ مَن يريد أن يتم تطبيق شريعة الله **عزّ** وجل، دعه إذاً يعلن ولاءه لهذا الخليفة. الله **عزّ** وجل قد ميّز الآن بين الصادق والكاذب.[14]

الطلبات والشهادة الشخصيّة

في حين لا تستخدم الدولة الإسلامية في العراق والشام (ISIL) بشكلٍ مميّزٍ الحديث الشخصي الذاتي باعتماد ضمائر المتكلّم المفرد، إنّها وجبهة النُصرة تستخدمانه جنباً إلى جنب مع الطلبات الشخصية بين الأفراد، وذلك على سبيل المثال في نوعٍ من الشهادة المُقنعة:[15]

> إنّ ما أذكره **أنا** من حقائق، أشهد عليه **أنا**. سوف أؤكّد **أنا** على ما رأته عينـي، وما سمعته أذنـيّ، وما أدركه **قلبـي**، وسأخبرك **أنا** بما علمته من آخرين. أنا أطلب منك، باسم الله، لا إله إلا الله، أن تنقل هذا الحديث إلى الشيوخ والقادة في الشام [سوريا] وأماكن أخرى.[16]

جبهة موحّدة

تمثّلت حالةٌ كامنةٌ مهمّة أخرى في تواصلات المجموعتين على حدّ سواء بالجمع بين الوعود الاجتماعية والحديث الشامل باعتماد "ضمائر جماعة المتكلّمين/ضمائر جماعة

---

[13] بخلاف ذلك، لم تستخدم أنصار الشريعة وتنظيم القاعدة في شبه الجزيرة العربية (AQAP) هذه الاستراتيجية.

[14] ترد **الشدّة** بالخط العريض، والمشاعر والقِيَم الإيجابية بالخط المائل، في حين يتم وضع خطّ تحت الحديث المستقبلي.

[15] تُعتبر هذه الاستراتيجية غائبة في حديث تنظيم القاعدة في شبه الجزيرة العربية (AQAP) على وسائل التواصل الاجتماعي.

[16] يرد **الحديث الذاتي** بالخط العريض، في حين يرد التوجّه إلى الآخرين والطلب منهم بالخط المائل.

المتكلّمين الدالّة على الملكيّة". غالباً ما يتكرّر هذا الحديث (علامةٌ مميّزة للصُدْق في الخطاب العربي) ويعتمد إلى درجة كبيرةٍ على فكرة إعلان البيعة والولاء:

> باسم الله الرحمن الرحيم، الدولة الإسلامية، والنعمة من الله أبو بكر البغدادي، **نحن جميعاً** نعلن ولاءنا له، أمير الدولة دولت**نا** مُنتصرة! باسم الله الرحمن الرحيم، الدولة الإسلامية، والنعمة من الله أبو بكر البغدادي، **نحن جميعاً** نعلن ولاءنا له، أمير الدولة دولت**نا** مُنتصرة! إنّهم يقاتلون من أجل النصر! إنّهم يرغمونهم على الانحناء مُستخدمين مدافع الهاون و[رشاشات] بي كاي سي (PKCs). دولت**نا** مُنتصرة! الدولة الإسلامية، والنعمة من الله أبو بكر البغدادي، **نحن جميعاً** نعلن ولاءنا له، أمير الدولة دولت**نا** مُنتصرة! أيّها المسلمون، هل أنتم مستعدّون؟ بعد المعاناة لمئات السنوات، ستحصلون على الحرّيّة. دولت**نا** مُنتصرة![17]

تتمثّل نقطتنا الرئيسية التي يتوجّب استخلاصها من هذا التحليل لإثبات المفهوم بأنّ ذلك التحليل المرتكز إلى الحاسوب لمجموعات كبيرة من بيانات وسائل التواصل الاجتماعي يمكن أن يوفّر رؤية من حيث تقنيات التجسس وإجراءاته حول عمليات المعلومات (IO) فيما يتعلّق برسائل الخصوم. في هذه الحالة، يُعتبر تحديد استراتيجيات التوعية والحُجج خطوة تفسيرية قد تُثير الرسائل المضادة.

تحليل الصور المُمكنن: المصادر الخارجية لفهم بيئة المعلومات

تجمع هذه المقاربة بين تحديد الموقع الجغرافي لمصادر البيانات وبرمجيات تصنيف الصوَر وتعيين المواقع على الخرائط من أجل تصنيف الصور ورسم خرائط لها آلياً في مجموعات كبيرة من بيانات وسائل التواصل الاجتماعي. في نهاية المطاف، يوفّر ذلك للقادة القدرة على رؤية أفكار المجموعات المحليّة التي تستحقّ أن يتم تبادلها (مثلاً، صوَر الشاحنات، والأزياء الرسمية، والميمات والرسوم المتحرّكة) وأين يتم تبادلها جغرافياً: ما الذي يريد أشخاصٌ موجودون في موقعٍ محدّدٍ تبادله مرئياً على وسائل التواصل الاجتماعي (بودين–بارون، مارسيلينو وآخرون [Bodine–Baron, Marcellino et al.]، 2015)؟ في حين تحاول المقاربات الأخرى التي جرى وصفها في هذا الفصل حلّ مشكلة الخرطوم (أي تدفقات النصوص الآنية غير المُفرزة) — بيانات نصيّة أكثر بكثير مما يمكن لمحلّلين بشريين قراءته — يقوم هذا الأسلوب بالأمر نفسه بالنسبة للبيانات المرئية، وهو نوع من البيانات نتوقّع أنّ حجمه سيبقى آخذاً بالزيادة مع زيادة تغلغل الهواتف الجوّالة وقدرة الشبكة عبْر الكرة الأرضيّة. نعتقد أنّ هذه المقاربة تقترن بقدرةٍ كامنةٍ كبيرة للأسباب التالية:

---

[17] ترد العلاقات الشاملة **بالخط العريض**، في حين ترد الوعود بالخط المائل.

- إنّها شكلٌ منخفض الكلفة من جمع البيانات عن بُعْد والذي لا يشكّل تهديداً لأصول أخرى.
- تستغلّ تدفّقاً إضافياً من البيانات الذي يجب أن ينمو مع تغلغل وسائل التواصل الاجتماعي المتزايد.
- تُحرّر وقت تحليل الخبراء البشريين وانتباههم.
- يمكن أن تكون الصُور غنيّة بالمعلومات الثقافيّة وأن تكون قيّمةً بشكلٍ خاصّ في المناطق التي تتمتّع بمعدّلات منخفضة من الإلمام بالقراءة والكتابة.
- إنّها طريقة لتحديد المصادر الخارجية لما يهمّ في بيئة المعلومات: إنّها تحدّد جغرافياً موقع الصور التي ترى المجموعات المحليّة أنها تستحقّ أن يتم تبادلها.

نشير إلى أنّ هذا مثلٌ جيّدٌ عن التمييز بين عمليات المعلومات (IO) وعمل الاستخبارات. يمكن استخدام هذا الأسلوب بوصفه جزءاً من عمليات التأثير (ما هي المخاوف الثقافيّة والسياسيّة لعامّة الجمهور المحليّ؟)، ولكن يمكن استخدامها بالسهولة نفسها لجمع معلومات استخباراتيّة حول ساحة المعركة (أين نرى أنّه يتم تبادل المزيد من صور الدبابات، والشاحنات، والأسلحة، والأزياء الرسميّة؟). إنّ ما يميّز هذا بوصفه جهداً لعمليات المعلومات قد لا يكون الأسلوب، ولكن، بدلاً من ذلك، الأسئلة المطروحة والنيّة منها.

الخطوة 1: جمع بيانات وسائل التواصل الاجتماعي المُحدَّدة جغرافياً

تتمثّل الخطوة الأولى في هذه المقاربة بجمع بيانات وسائل التواصل الاجتماعيّ المحدّدَة الموقع من خلال إمّا إضافة الوسم الجغرافي أو الاستدلال الجغرافي.[18] يتمتّع الخياران على حدّ سواء بمزايا:

- إنّ استخدام البيانات التي تحمل وسماً جغرافياً فحسب يمنح المستوى الأعلى من الثقة بدقّة الموقع والمستوى الأعلى من تفصيل الموقع على حدّ سواء. يمكن أن نعلم بثقة وبالتحديد من أين تأتي بيانات وسائل التواصل الاجتماعي ويمكننا رسم خريطة لذلك الموقع مع تبسيطها إلى مستوى وحدات التحليل المحتملة (مثلاً، المدن أو الأحياء). على الرغم من ذلك، بما أنّ أغلبيّة بيانات وسائل التواصل الاجتماعي لا تحمل وسماً جغرافياً، قد يحدّ هذا الخيار كميّة البيانات المتوفّرة للتحليل. ولأنّ السائحين يميلون إلى تشغيل ميزة تحديد الموقع الجغرافي على أجهزتهم الجوّالة، من الممكن أن تؤدّي صورهم إلى تحيّز العيّنة.

[18] نلاحظ اختلافاً كبيراً على المستوى الوطني في تغلغل الهواتف الجوّالة، وفي حجم البيانات التي تحمل وسماً جغرافياً/القابلة للاستدلال الجغرافي. وبالتالي، قد تكون هذه المقاربة أكثر أو أقلّ عمليّةً في أجزاء مختلفة من العالم.

- يمكن أن يلتقط الاستدلال الجغرافي (مثلاً، باستخدام اسمي المدينة والمحافظة على حدّ سواء في حقل موقع المُستَخدِم) المزيد من البيانات على مستوى عالٍ من دقّة تحديد الموقع الجغرافي. على الرغم من ذلك، يُعتبر تفصيله محدوداً. في المثل المذكور سابقاً حول تعقّب انتشار الرسائل على وسائل التواصل الاجتماعي المصريّة، كان معدّل الدقّة البالغ 80 في المئة على مستوى المناطق الوطنيّة فحسب.

من مجموعة بيانات وسائل التواصل الاجتماعي هذه، يمكن تجريد مُعرّفات الموارد المحدّدة (URLs) الخاصّة بالصور، ويمكن جمع بيانات الصور من البيانات الوصفيّة للموقع، ما يُخلّف كومةً كبيرةً وغير مُفرزة من الصور التي شعرت مجموعةٌ محليةٌ أنها تستحق أن يتم تبادلها. وتتمثّل الخطوة الثانية باستخدام الأدوات الآليّة من أجل فرز هذه الصور وتصنيفها.

الخطوة 2: تصنيف الصور المُمكنن

تتمثّل الخطوة الثانية باستخدام برمجيات تصنيف الصور على مجموعة بيانات الصور. بتاريخ تأليف هذا التقرير، كانت الشبكات العصبيّة العميقة (DNNs) أسلوباً واعداً لتقسيم الصور إلى طبقات مستخلصة متعددة، مع تحذيرين:

- **قوّة المعالجة.** على عكس الأساليب التحليليّة الخاصة بالنصوص التي تمت مناقشتها سابقاً، يُعتَبر تصنيف الصور مُهمّةً تتطلّب وقتاً وجهداً من الناحية الحاسوبية، كما تتطلّب، لتكون مُجدية، مصفوفات حوسبة متوازية (على عكس نظام حاسوب مكتبي واحد). في مثلنا، نتج عن جمع صور تحمل وسماً جغرافياً متبادلَة على تويتر (Twitter) وفيسبوك (Facebook) في أنحاء أفريقيا عام 2015 على مدى أسبوعين 283,000 صورة. تطلّب ذلك حوالي ثلاثة أيام من الحوسبة المتوازية للمعالجة.
- **دقّة التصنيف.** ثمّة توتر بين دقّة تصنيف الصور وتفصيله. على مستوى منخفض من التفصيل (مثلاً، "المركبات")، تُعتبر التكنولوجيا الحالية عالية الدقّة. وإنّما على مستويات أعلى من التفصيل (مثلاً، "الدبابات" و"الشاحنات")، تتراجع الدقّة.

الخطوة 3: تحديد مواقع الصور على الخرائط

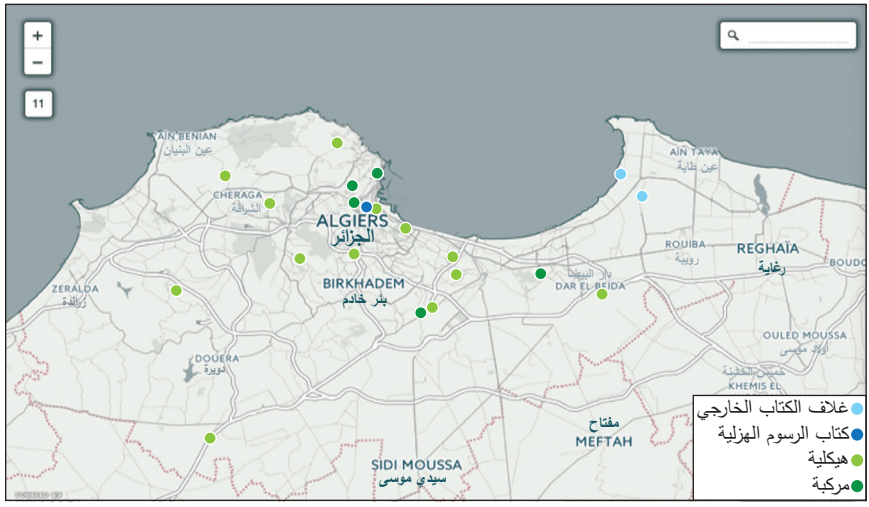
تتمثّل الخطوة النهائية بتحديد موقع هذه الصور على الخرائط باستخدام برمجيات رسم الخرائط من أجل تجسيد الأمور التي تقوم المجموعات المختلفة بتبادلها تجسيداً مرئياً. ولأنّ هذه البيانات تكون مطبوعة بالوقت، يمكننا أيضاً رؤية التغيّرات مع الوقت. كتوضيح لكيفية التمكّن من استخدام هذا دعماً لعمليات المعلومات (IO)، أُنظُر في كيفية تمكّن الصور من الإشارة إلى قضايا اجتماعية ثقافية وسياسية وتجسيدها في بعض

الأحيان. في التحليل الذي تتم مناقشته في هذا القسم، وجد المُصنِّف عدداً من "كُتُب الرسوم الهزلية" التي اتّضح في النهاية أنّها رسوم متحرّكة سياسيّة.[19] قد يكون لتلك ولأصناف أخرى من الصور قيمةٌ كبيرةٌ في رسم خريطة لبيئة المعلومات المحليّة وإظهار ما الذي تختار عامّة جمهور تبادله مرئياً ومن أين تتبادل هذه الصُور.

إنّ الشكل رقم 3.4 هو لقطة عن أداة الشبكات العصبية العميقة (DNN) تُظهر صوراً تم الكشف عنها آلياً، والتي تم تحديد موقعها على الخريطة بحسب الصنف (رسوم متحرّكة سياسية، مبانٍ ومركبات) وتحديد الموقع الجغرافي، من أجل تشكيل خريطة لتبادل الصور.

إنّ التمكّن من تجسيد أين وعلى أي مستويات من الكثافة تتم "مناقشة" مخاوف مجموعة مرئياً قد يكون طريقةً قويةً لفهم الديناميكيات داخل بيئة المعلومات واستغلالها.

الشكل رقم 3.4
الصور المُتبادَلة، بحسب النوع والموقع الجغرافي



المصدر: بودين–بارون، مارسيلينو وآخرون (Bodine–Baron, Marcellino et al.)، 2015.

RAND *RR1742-3.4*

[19] يسلّط هذا الضوء على بعض الحدود الحاليّة لبرمجيات تصنيف الصور. في حين تُعتبر كُتُب الرسوم الهزلية والرسوم المتحرّكة السياسيّة نوعين مختلفين جداً بالنسبة للبشر، إنّهما يتشاركان ميزات مرئية مماثلة. تستخدم الآلات ميزات مختلفة ولها بالتالي أوجه استخدام وقيود مختلفة.

السياق والاعتبارات لاستخدام تحليل وسائل التواصل الاجتماعي في عمليات المعلومات

استخدم الفصلان السابقان القدرات المرتبطة بالمعلومات (IRCs) بوصفها إطار عمل للتفكير في قيمة تحليل وسائل التواصل الاجتماعي في عمليات المعلومات (IO) ونقاط إدراجها. قدّما أيضاً مقاربات تحليليّة نموذجيّة من أجل نقل نطاق الاحتمالات ضمن تحليلات بيانات وسائل التواصل الاجتماعي وقوّة عمليات المزج المبدعة بين الأساليب. ننتقل الآن إلى السياق الأوسع لجهدٍ تبذله وزارة الدفاع الأمريكيّة (DoD) من أجل تطوير القدرة التحليلية الخاصّة بوسائل التواصل الاجتماعي. وكما نناقش في هذا الفصل، يعكس القانون الأمريكي القائم بشأن جمع البيانات من قِبَل وزارة الدفاع الأمريكيّة التكنولوجيا من حقبةٍ سابقة، وثمّة حالة من عدم الوضوح بشأن الأمور التي يستطيع ممارسو عمليات المعلومات القيام بها وتلك التي لا يستطيعون القيام بها بالتحديد فيما يخصّ بيانات وسائل التواصل الاجتماعي. بالنسبة لما يتجاوز الحدود القانونية الصارمة، ثمّة قضايا أخلاقية يجب أخذها بعين الاعتبار، وفي عالمٍ ما بعد سنودن (Snowden) حيث **يشعر** الجمهور الأمريكي بالقلق بشكلٍ عامٍ إزاء قضايا الخصوصية وجمع البيانات الحكومية، يُعتبر الوضوح حول ما يشكّل سلوكاً قانونياً وأخلاقياً أساسياً لأي جهد لتحليل وسائل التواصل الاجتماعي. يشمل السياق لتطوير قدرة وزارة الدفاع الأمريكيّة على تحليل وسائل التواصل الاجتماعي اعتبارات عمليّة — بالتحديد، كلفة جمع البيانات وتحليلها، والاستحواذ على التكنولوجيا، والتدريب.

لدى معالجة هذه التحديّات المتنوّعة في وجه استخدام تحليل وسائل التواصل الاجتماعي دعماً لعمليات المعلومات، نقرّ بأنّها (وتصبح بشكلٍ متزايدٍ) مترابطة. تعتمد مراجعتنا للأبحاث ذات الصلة على الدراسات السابقة الخاصّة باستخدام وسائل التواصل الاجتماعي والدراسات السابقة حول عمليات المعلومات بشكلٍ واضحٍ على حدّ سواء؛ إنّ أغلبية ما يُعتبر قابلاً للتطبيق على عمليات المعلومات بشكلٍ عام، هو قابل للتطبيق على تحليل وسائل التواصل الاجتماعي بشكلٍ خاص. ونعتمد أيضاً على الدراسات السابقة من أوساط الأبحاث الأكاديمية التي تحاول بحدّ ذاتها التعامل مع مشكلة حداثة وسائل التواصل الاجتماعي.

القضايا القانونية

يجب أن يبدأ أي اعتبار لشرعيّة بناء قدرة على تحليل وسائل التواصل الاجتماعي أو استخدامها من التفاوت بين **الابتكار وتنظيم الابتكار**. تواجه وزارة الدفاع الأمريكيّة (DoD) والباحثون المدنيون التحدّي نفسه:

> بما أنّ تنظيم التكنولوجيات الجديدة يمكن أن يكون عملية بطيئة، يشكل تقييم الأنظمة القانونية ذات الصلة في مجال البحث هذا تحدّيات. يُعَرِّض نقص التوجيه القانوني الخاصّ بالتكنولوجيات الجديدة المُجيبين بشكلٍ محتمل للخطر ويترك لدى الباحثين أسئلة من دون إجابات. أُنظُر مثلاً في مُقيمٍ أمريكيٍّ تمّ الاتصال به للمشاركة في بحث عَبْر وسائل التواصل الاجتماعي في الوقت الذي يتواجد فيه خارج الولايات المتّحدة. هل ينطبق القانون الأمريكي، أو القانون الساري المفعول في البلد الذي يتواجد فيه المُجيب، أو قانون البلد الذي تقع فيه مؤسسة البحث؟...
>
> في غياب توجيه قانوني واضح، يحتاج الباحثون إلى تنظيم أنفسهم ... من أجل استيعاب قابلية نقل المنصّة التي نرغب بإجراء البحث عليها ومرونتها من أجل عدم التسبب بتآكل حماية المشاركين في البحث (مورفي وآخرون [Murphy et al.]، 2014، ص. 38–39).

نلاحظ فجوةً بين وزارة الدفاع الأمريكيّة والمناظير التجارية حول تحليلات بيانات وسائل التواصل الاجتماعي. في مقابلاتنا مع الخبراء حول جمع بيانات وسائل التواصل الاجتماعي وتحليلها التجاريين، أبلغ الذين جرت مقابلتهم عن مخاوف قليلة بشأن جمع البيانات في سياقات تجارية أو لدى جمع بيانات حول مواطنين أمريكيين أو داخل الولايات المتحدة. ركّزت المخاوف على المعلومات المرتبطة بالصحّة والتي تحظى بالحماية بموجب قانون إخضاع التأمين الصحي لقابلية النقل والمحاسبة (Health Insurance Portability and Accountability Act) والمعروف بالمقتطع الهجائي HIPAA) وأي بيانات قد لا تريد شركة تبادلها في خلال مرحلة اكتشاف الأدلّة بشأن دعوى قضائية (مقابلة مع خبير متخصّص في الموضوع، 31 أغسطس/آب 2016).

في حين تواجه وزارة الدفاع الأمريكيّة تحديّات مماثلة فيما يتعلّق بجمع بيانات وسائل التواصل الاجتماعي وتحليلها، إنّها ليست في موقع ملائم لتنظيم نفسها. بدلاً من ذلك، يتوجّب عليها أن تتقيّد بدقّة بإطار عمل قانوني وخاص بالسياسات لم يواكب الظروف الحالية. يشكّل الامتثال لعقود حكوميّة مشكلةً مهمّةً بالنسبة للشركات التجارية، بالنظر إلى القيود المفروضة على جمع المعلومات المُحدِّدة للهويّة الشخصيّة والقيود الأكثر صرامةً بَعْد المفروضة على البيانات التي يتم جمعها حول المواطنين الأمريكيين.

قد يقيّد ذلك إلى حدّ كبير القدرة على جمع المعلومات الاستخباراتية. فعلى سبيل المثال، تشمل اللوائح مجموعة واسعة من المعلومات، بما فيها رقم الضمان الاجتماعي الخاص بفرد، وتاريخ ولادته وبصمات أصابعه وبيانات بيومترية أخرى (توجيه وزارة الدفاع الأمريكية رقم 11.5400 5400.11 [DoD Directive]، 2014).

القانون الأمريكي الحالي وعمليات المعلومات

يحاول القانون والسياسات الأمريكية الحاليّة الامتثال بشكلٍ تماثليٍّ للمعاهدات الدوليّة التي لم يتم تصميمها لعمليات المعلومات (IO) والطرق الحديثة لجمع المعلومات الاستخباراتية دعماً لعمليات المعلومات، مثل تحليل وسائل التواصل الاجتماعي (هوليس [Hollis]، 2009؛ جوريش [Jurich]، 2008).[1] وبالتالي، يجب أن تأخذ أي محاولة لتنفيذ قدرةٍ على تحليل وسائل التواصل الاجتماعي مُمتثلة قانونياً ما يلي بعين الاعتبار.

عدم اليقين بشأن نقل القانون الأمريكي إلى عمليّات المعلومات (OI) وتطبيقه عليها

يُعدّ عدم اليقين هذا زاجراً للقادة للانخراط في عمليات المعلومات (IO). وما يُعقّد الوضع أكثر هو أنّ الأبحاث القائمة حول عمليات المعلومات قد مالت إلى افتراض الحرب المرتكزة إلى الدول وتجاهل عوامل أخرى، مثل الجهات الفاعلة غير الحكومية أو العدوان من قِبَل جهات فاعلة مرتبطة بالدول تحت عتبة الحرب (مثلاً، دعاية الدولة الإسلامية في العراق والشام [ISIL] وجهود التجنيد التي تبذلها، متصيّدو "الإنترنت" في روسيا الذين يتقاضون أجراً) (دونكان [Duncan]، 2015).

في الحرب التقليديّة مع أنظمة أسلحةٍ تقليديّة، يُعتبر القانون القائم واضحاً في تمييزه بين الأهداف المدنية مقابل الأهداف العسكرية وما يُشكّل "استخدام قوّة" قانونيّاً. لدى الانخراط في صراعات خارج إطار الأعمال العدائيّة المُعلنة أو استخدام قدرات غير

---

[1] تشمل هذه المعاهدات الدولية إعلان سانت بطرسبرغ لعام 1868 (St. Petersburg Declaration 1868) الذي يعلن "القوات العسكرية" بوصفها الشيء القانوني الوحيد للحرب؛ بند مارتنز من اتفاقيات جنيف لعام 1949 (Geneva Conventions' Martens Clause 1949) الذي يحدّد أن السلوك الذي لا يكون محظوراً في الحرب ليس مسموحاً بالضرورة؛ الحظر الذي ينصّ عليه ميثاق الأمم المتحدة (United Nations Charter) بشأن استخدام القوة أو التهديد باستخدامها خارج الدفاع عن النفس خلال "صراع مسلّح" ومبدأ "التمييز المدني" الذي يُحظّر العمليات العسكرية ضدّ الشعوب المدنيّة، والممتلكات والبنى التحتية؛ والمادة IV من معاهدة الفضاء الخارجي (Outer Space Treaty) التي تتطلّب استخدام الفضاء "لأغراض سلمية حصرياً" (هوليس [Hollis]، 2009). تمّت كتابة هذه المعاهدات جميعها مع أخذ استخدام القوّة الحركية العسكرية بعين الاعتبار، وليس عمليات المعلومات (IO) العسكرية.

أنظمة الأسلحة التقليدية، تزول أغلبية هذا الوضوح. لدى استهداف بنى تحتية مزدوجة الاستخدام (مثلاً، أنظمة الاتصالات، منصات وسائل التواصل الاجتماعي)، كيف يميّز القادة بين المقاتلين وغير المقاتلين؟ هل تشكّل مكافحة الدعاية استخداماً للقوّة؟

وأخيراً، يُستمدّ القانون الأمريكي بخصوص عمليات المعلومات (IO) بشكلٍ تماثليٍّ من قانون الحظر الذي يحكم الصراع المسلّح التقليدي — والذي يركّز على الأمور التي لا يجوز القيام بها، وليس على تلك التي يجوز القيام بها. تُضعف هذه الهيكلية القانونية القدرة الإنتاجيّة في عمليات المعلومات (هوليس [Hollis]، 2009، ص. 16). في عصر التبادل العالمي الفوري من وسائل الإعلام التقليدية ("تأثير شبكة سي.أن.أن" ["CNN effect"]) ووسائل التواصل الاجتماعي على حدّ سواء، يملك القادة أسباباً قويةً لتجنّب استخدام القدرات المرتبطة بالمعلومات (IRCs) بطرقٍ جديدةٍ أو مختلفة (هوليس [Hollis]، 2009).

التعقيد في الطبقات المتداخلة من القانون والسياسات التي قد يتم تطبيقها على عمليات المعلومات (IO) والقدرات المرتبطة بالمعلومات (IRCs)

يمكن تطبيق القوانين الدوليّة بشأن مقاضاة الصراع المسلّح (مثلاً، اتفاقيات جنيف [Geneva Conventions] وميثاق الأمم المتحدة [United Nations Charter]) بشكلٍ محتمل. قد تستهدف حملات عمليات المعلومات (IO) أو تعتمد على أنظمة ومنصات الاتصالات الفضائية وبالتالي، يجوز تطبيق قانون الفضاء الدولي. يحظّر دستور الاتحاد الدولي للاتصالات (Constitution of the International Telecommunications Union) "التدخّل الضار" في أنظمة اتصالات أمم أخرى (مع استثناء تركيبات الرادارات العسكرية، التي قد تعني ضمناً أو قد لا تعني ضمناً مجموعة أوسع من تكنولوجيا الاتصالات العسكرية). يتمثّل الأمر الأكثر صعوبةً بالفجوة بين القانون الأمريكي الداخلي والقوانين الداخلية في بلدان أخرى. في حال إجراء وزارة الدفاع الأمريكية (DoD) عمليات معلومات (IO) قد تشمل على سبيل المثال حملةً للطعن في موثوقية قائدٍ متطرّف يعيش في بلدٍ آخر، قانون أي بلد يجب تطبيقه؟ قد تشمل هذه الحملة بالفعل جمع بيانات وسائل التواصل الاجتماعي وتحليلها. من جديد، قد يُثني التعقيد في أطر العمل القانونيّة القادة عن استخدام القدرات المرتبطة بالمعلومات (IRCs) تحقيقاً لأقصى قدرتهم (هوليس [Hollis]، 2009).

أوجه القصور في القانون بخصوص عمليات المعلومات (IO) عندما ينطوي على جهات فاعلة غير حكومية

لا تزال الجهات الفاعلة الحكومية (مثلاً، روسيا والصين) ذات صلة في الحرب وعمليات

المعلومات (IO). على الرغم من ذلك، وبتاريخ تأليف هذا التقرير، كان التركيز في القتال في الحرب على الصراع غير المتماثل مع الجهات الفاعلة غير الحكومية، مثل الدولة الإسلامية في العراق والشام (ISIL). تُعتبر حالة حرب المعلومات جذّابةً بشكلٍ خاص بالنسبة للجهات الفاعلة غير الحكومية لأنّها رخيصة، ويمكن الوصول إليها ولها مُتناوَل عالمي على عكس العمليات الحركيّة التقليدية. ولكنّ القوانين الداخلية والدولية القائمة غير كافية لمعالجة مثل هذه الصراعات. في ما يتجاوز الرعاية الحكومية الواضحة لمجموعة متطرّفة، تُعتبر الولايات المتحدة مقيّدة في كيفيّة التمكّن من الردّ مباشرة. قد لا تشكّل مثلاً جهود الدعاية لاكتساب المجنّدين أو جمع الأموال هجمات مسلّحة وقد لا تفي بالتالي بعتبات الدفاع عن الذات الأمريكية ([Hollis]، 2009).

يشكّل عدم يقين القوانين الأمريكية والدوليّة بخصوص عمليات المعلومات وتعقيدها وأوجه القصور فيها زواجر للجيوش للانخراط في مثل هذه العمليات، وقد تجعل هذه العوامل مسؤولاً في مكتب المشاور العدلي العام يتردد في تأييد شرعيّة استخدام مقترح للقدرات المرتبطة بالمعلومات (IRC) بثقةٍ. إنّها مشكلة مثيرة للتهكّم وللاستياء بشكلٍ خاص بالنظر إلى قدرة عمليات المعلومات على تحقيق الأغراض العسكرية والسياسية بضرر أقلّ من حرب تقليدية (هوليس [Hollis]، 2009).

وصف خبراء متخصصون في تحليل وسائل التواصل الاجتماعي التابعون لوزارة الدفاع الأمريكية (DoD) والذين قابلناهم القانون الأمريكي بخصوص جمع المعلومات المُتاحة للعامّة على أنّه بالٍ من حيث الإجراءات والسياسات على حدّ سواء، بحيث يعكس طُرُق حقبة الحرب الباردة (Cold War) وأنواع البيانات الخاصة بها. لاحظوا أنّه يتوجّب على وزارة الدفاع الأمريكية إجراء مراجعة قانونية لإزالة المناطق الرماديّة في السياسات المرتبطة بوسائل التواصل الاجتماعي، وتطوير سياسات أوضح تعكس الظروف الحالية، ووضع برامج مُدرجة على الموازنة على مستوى الخدمة لوضع هذه السياسات حيّز التنفيذ.

المخاوف المرتبطة بالباب 10 مقابل تلك المرتبطة بالباب 50

يحدّد البابان 10 و50 من قانون الولايات المتحدة الأمريكيّة الأدوار والمسؤوليات الخاصّة بالجيش الأمريكي وأجهزة الاستخبارات الأمريكية، على التوالي (وول [Wall]، 2011). يوفّر البابان السلطة القانونية للعمليات العسكرية بموجب نشاطات وزارة الدفاع الأمريكية (DoD) والاستخبارات والأعمال السرّية التي تضطلع بها وكالات الاستخبارات ويميّز بينها. يتوجّب على قيادات الجيش الأمريكي التي تنخرط في عمليات المعلومات (IO) أن تعمل وفقاً لما هو مسموح به بموجب الصلاحيّات المنصوص عليها في الباب 10. بالنسبة للقدرات المرتبطة بالمعلومات (IRCs) القائمة منذ وقتٍ أطول والتي قد تَمرّ

عبر أحكام الباب 10 والباب 50 (مثلاً، المسائل الإلكترونية)، ثمّة نماذج يتم بموجبها التنسيق بين الصلاحيّات المنصوص عليها في الباب 10 والباب 50 مع إشراف مناسب. على سبيل المثال، إنّ القوة الجوية الرابعة والعشرين (24th Air Force) منظّمة لإجراء عمليات مع التحرّك بخفّةٍ ذهاباً وإياباً بين البابين. ينسّق مقاتلو الحرب المعنيون بالباب 10 مع وكالة الأمن القومي (National Security Agency [NSA]) من أجل اكتساب إمكانية الوصول إلى استخبارات الإشارات بموجب صلاحيّة وكالة الأمن القومي المنصوص عليها في الباب 50. لدى القوة الجوية الرابعة والعشرين أيضاً وحدات بموجب الباب 10 مع "توجيه أمريكي لاستخبارات الإشارات" (U.S. Signals Intelligence Directive [USSID]) والذي يعرّف الحدود والعمليات التي تستخدمها من أجل جمع استخبارات الإشارات تحت إشراف وكالة الاستخبارات والمراقبة والاستطلاع التابعة للقوى الجوية (Air Force Intelligence, Surveillance, and Reconnaissance Agency) وسلطة وكالة الأمن القومي. تتنقّل هذه الوحدات بانتظامٍ بين الاضطلاع بالمهام بموجب السلطات التي ينصّ عليها البابان 10 و50 (فوترينو [Vautrinot]، 2012).

يُعتبر تخطيط عمليات المعلومات واستخدام القدرات المرتبطة بالمعلومات واللذين ينطويان على وسائل التواصل الاجتماعي وتحليلات بيانات وسائل التواصل الاجتماعي جديدين بالمقارنة مع النشاطات الإلكترونية القائمة ولا يوجد أمثلة واضحة قابلة للمقارنة. قد تواجه القيادات التي تحاول بناء قدرة على تحليل وسائل التواصل الاجتماعي تدقيقاً خاصّاً لأنّ النشاطات المسموح بها بموجب الباب 10 والصلاحيات المنصوص عليها في الباب 50 قد تبدو متشابهة جداً: "يملك الجيش ووكالات الاستخبارات على حدّ سواء السلطة القانونية لإجراء نشاطات جمع المعلومات الاستخباراتية التي قد تعجز 'العين المجرّدة' عن رؤيتها" (وول [Wall]، 2011، ص. 91).

إذاً، في حين تملك قيادات الجيش السلطة القانونية لإجراء نشاطات عمليات المعلومات — وهي نشاطات قد تبدو للوهلة الأولى سريّة بموجب الباب 50 — أدّت عوامل تاريخية وسياسيّة إلى تدقيقٍ متزايد. وتتمثّل قضية تاريخية بمشكلة التقارب بين العمليات العسكرية والاستخباراتية في حقبة ما بعد عمليات 11 سبتمبر/أيلول (تشيسني [Chesney]، 2012). ويحصل ذلك على الرغم من البُنيان القانوني الذي يحكم العمليات المنصوص عليها في الباب 10 والباب 50 والذي، بشكلٍ مثالي، "يعمل من أجل التوفيق بين الرغبة في المرونة والسرعة والسريّة في السعي وراء تحقيق أهداف الدفاع القومي والسياسات الخارجية من جهة، والرغبة في المحافظة على درجةٍ هادفةٍ من المحاسبة الديموقراطية والامتثال لسيادة القانون من جهةٍ أخرى" (تشيسني [Chesney]، 2012، ص. 540). يجب أن يستعدّ الجيش الأمريكي للتغيّرات في التحدّيات التشغيلية والاستراتيجية التي يواجهها ويجب أن تتغيّر أنماط البُنيان القانوني رداً على ذلك.

يُعقّد هذا التفاوت بين الظروف التشغيلية المتغيّرة وأنماط البُنيان القانوني الوظيفة المشروعة لإشراف الكونغرس. في حين قد لا تبدو نشاطات عمليات المعلومات للوهلة الأولى أنّها تتوافق مع الأفكار التقليدية للنشاطات العسكرية، لا تتعدّى هذه النشاطات، مثل رصد وسائل التواصل الاجتماعي، على الباب 50:

> إنّها هيكلية الإشراف القديمة الخاصة بالكونغرس وسوء فهم القانون المصاحب اللذان يلقيان بظلالٍ من القلق وعدم المشروعية المزعومة على العمليات العسكرية المشابهة للنشاطات التي تجريها وكالات الاستخبارات. إنّ رؤية الكونغرس لعمليات الأمن القومي من حيث مسارات نقل المعلومات متباينة قانونياً وخطيرة تشغيلياً لأنها تشير إلى أنّ السلطات القانونية تستبعد كل واحدة منها الأخرى وتؤدي إلى مخاوف بشأن التعاون بين الوكالات بالتحديد في الوقت الذي يتوجب على هيكيلات السياسات والهيكليات القانونية التابعة لنا أن تشجّع التنسيق والتعاون المتزايدين بين الوكالات في وجه تهديدات الأمن القومي المترابطة (وول [Wall]، 2011، ص. 92).

ليست الطريقة للتمييز بين النشاطات المنصوص عليها في الباب 10 وتلك المنصوص عليها في الباب 50 بحسب النشاط بحدّ ذاته، وإنّما بدلاً من ذلك بحسب المعيار القانوني "للقيادة والمراقبة، بالإضافة إلى التمويل والسياق والنية من المهمة" (وول [Wall]، 2011، ص. 109). ويتجسّد مثلٌ عن نشاطٍ عسكريٍ مشروعٍ مسموحٍ به بموجب الباب 10 بجهد عمليات دعم المعلومات العسكرية (MISO) من قِبَل وحدات عسكرية، تعمل تحت سلسلة القيادة العسكرية خلال عمليات المساعدة الإنسانيّة/الإغاثة في حالات الكوارث، بنيّة تعزيز سلامة القوات الصديقة من خلال إقناع عامة الجماهير المحلية بنيّتها الحسنة.

تطوير توجيهات واضحة في السياسات حول استخدام وزارة الدفاع الأمريكية (DoD) لبيانات وسائل التواصل الاجتماعي

بالنظر إلى عدم اليقين هذا بشأن الاستخدام القانوني لعمليات المعلومات (IO) عَبْر طيف العمليات العسكريّة، وبالنظر إلى التفسيرات المتضاربة لما يشكّل نشاطات منصوص عليها في الباب 10 مقابل ما يشكّل نشاطات منصوص عليها في الباب 50، تحتاج وزارة الدفاع الأمريكية (DoD) بوضوح إلى تبيان أوجه القصور في السياسات والقوانين الحاليّة. لم تتم صياغة القانون الأمريكي والقوانين الدولية الواجبة التطبيق لتأخذ بعين الاعتبار عمليات المعلومات والطرق التقنية الحديثة المُستَخدَمة في عمليات

المعلومات، مثل تحليل وسائل التواصل الاجتماعي. وبالتالي، يتمّ تطبيقها في السياسات بأحكامٍ غامضةٍ ومتماثلة. أقرّ الكونغرس بحاجة وزارة الدفاع الأمريكية غير الاستخباراتيّة لتشغيل واستغلال بيانات وسائل التواصل الاجتماعي والمعلومات الأخرى المُتاحة للعامّة لمجموعةٍ من النشاطات العسكرية التقليدية، بما فيها حماية القوّات والوعي حول فضاء المعركة (مجلس النواب الأمريكي [U.S. House of Representatives]، 2016، ص. 246).

تقترن هذه القضية بطابعٍ ملحٍّ خاصٍ بالنسبة لوزارة الدفاع الأمريكية حيث "أنّ نقص السياسات المُحدّدة بوضوح يعيق قدرة [وزارة الدفاع الأمريكية] ... على فهم المشاعر العدائية والرسائل السردية في مسارح الأعمال العدائية النشطة، بالإضافة إلى الرصد لتحديد البيئات غير المتساهلة والشبه المتساهلة ومجالات النشاط المستقبلي المحتمل" (مجلس النواب الأمريكي [U.S. House of Representatives]، 2016، ص. 246).

مع قيام وزارة الدفاع الأمريكية بتطوير سياسات أفضل، يتوجب عليها بالطبع احترام القيود الأخلاقية والقانونية الأمريكية المفروضة على جمع معلومات حول الأشخاص الأمريكيين ومشاهدتها ومعالجة المشاهدة العرضية لدى التواجد في فضاء معركة العدو.

اعتبارات خاصّة: جمع المعلومات حول الأشخاص الأمريكيين

يتمثّل تحدٍ خاصٍ من حيث جمع بيانات وسائل التواصل الاجتماعي دعماً لعمليات المعلومات (IO) بالحظر القانوني على جمع الاتصالات من أشخاص أمريكيين. يجب أن تمتثل نشاطات عمليات المعلومات الخاصّة بوزارة الدفاع الأمريكية (DoD IO) للقيود على العمليات الداخلية المنصوص عليها في الباب 10 (إلستاد [Elstad]، 2008)، بالإضافة إلى الأمر التنفيذي رقم 12333 الذي يُحظّر الاستحواذ على معلومات حول أشخاص أمريكيين وتخزينها وتعميمها (راجع المنشور المشترك 3-13 [JP 3-13]، 2014). إنّ إطار العمل القانوني الأمريكي الحالي، والمُصمّم من أجل حماية الخصوصية والحدّ من المراقبة الداخلية، "لم يتوقّع طبيعة التهديد الحالي للأمن القومي من الإرهاب العابر للحدود الوطنية، ولم يتوقّع أيضاً تطوّر شبكات التواصل العالمية أو الأساليب التقنية المتقدّمة لجمع المعلومات الاستخباراتية" (تايبال [Taipale]، 2007، ص. 130). وبشكلٍ أساسيّ، لم تتم صياغة إطار العمل القانوني الحالي ليأخذ بعين الاعتبار تداخل الاتصالات الداخلية والخارجية — وهو خاصيّة لوسائل التواصل الاجتماعي — وقد تشمل أيضاً المعلومات التي يتم جمعها بشأن عامة الجمهور في بلدٍ آخر أو حولها معلومات من أشخاص أمريكيين.

يؤدي ذلك إلى توقّع الجمع العرضي بطبيعته لمعلومات شخص أمريكي واتصالاته لدى الاضطلاع بعمليات أجنبية، وهو قيدٌ بالغ التشدّد مفروض على استخدام بيانات وسائل التواصل الاجتماعي. من الناحية العملية، ينتج عن الامتثال لإطار عملٍ قانونيٍّ مصممٍ من أجل منع التجسّس الداخلي تأثيرٌ خانقٌ على عمليات وزارة الدفاع الأمريكية، بحيث يفرض فترة زمنية مدّتها 90 يوماً على استخدام بيانات وسائل التواصل الاجتماعي والاحتفاظ بها، بالإضافة إلى حلولٍ بديلةٍ للأطراف الثالثة والتي قد تسلب من محلّلي وزارة الدفاع الأمريكيّة السياق المهمّ لفهم النتائج التحليلية.[2]

ليس مجدياً من الناحية التكنولوجيّة مَنْع الجمع العرضي بشكلٍ كامل، ولذلك يجب أن تكون سياسات عمليةٌ، وإنّما أيضاً مقبولة قانونياً وسياسياً قادرةً على تبيان أنّ الجهود المشروعة التي تهدف إلى جمع البيانات المُتاحة للعامّة والتي قد تشمل معلومات حول أشخاص أمريكيين لا تقوم بجمع بيانات حول أشخاص أمريكيين ولا تركّز عليهم.

القضايا الأخلاقية

لا يتوجّب فحسب على وزارة الدفاع الأمريكية (DoD) استيفاء عتبة قانونية في تحليل وسائل التواصل الاجتماعي، وإنما يتوجب عليها أيضاً استيفاء عتبة أخلاقيّة تعكس القِيَم الثقافية الأمريكية (بارتليت ورينولدز [Bartlett and Reynolds]، 2015). تدعو الحاجة بالتالي إلى صياغة مدوّنة أخلاقيات رسمياً لنشاطات الدفاع التي تنطوي على بيانات وسائل التواصل الاجتماعي. وبالأخصّ بالنظر إلى حداثة الابتكار في تحليلات بيانات وسائل التواصل الاجتماعي ووتيرته السريعة، لا بدّ من أن تكون هناك مسارات عمل لا تزال — في الوقت الذي ليست فيه محظورةً بشكلٍ صريحٍ بموجب السياسات أو القانون — تقترن بقدرةٍ كامنةٍ على انتهاك القِيَم القومية الأمريكية.

الأخلاقيّات في نشاطات البحث على الإنترنت

يمكن إنارة التحدّي في صياغة مدوّنة أخلاقيات صريحة لتحليل وزارة الدفاع الأمريكية (DoD) لوسائل التواصل الاجتماعي من قِبَل نقاش مماثل في الوسط البحثي المدني حول "نشاط البحث على الإنترنت" (ماركهام وبوشنان [Markham and Buchanan]، 2012). لدى الوسط البحثي الأكاديمي مدوّنات أخلاقيات رسمية وأنظمة رصد وإنفاذ

[2] على سبيل المثال، قد يكون ذلك مقاول من طرف ثالث يستحوذ على بيانات وسائل التواصل الاجتماعي ويخزّنها بالنيابة عن كيانات عمليات المعلومات التابعة لوزارة الدفاع الأمريكية (DoD IO)، مع تقديمها مع طبقة من البيانات المُجْتَزَأة من سياقها.

قائمة لحماية البحث البشري العام، ولكنّه وجد أنّ أخلاقياته وقواعده القائمة قد تخلّفت عن التقدّمات في هذا المجال. وأدّى ذلك إلى فجوة كبيرة بين ممارسات البحث على الإنترنت وممارسات الأخلاقيات. فعلى سبيل المثال، من بين المقالات المرتبطة بالبحث حول وسائل التواصل الاجتماعي البالغ عددها 382 مقالة والمنشورة بين عامي 2006 و2012، أربعة في المئة فقط نظرت في القضايا الأخلاقية وتداعيات استخدام تويتر (Twitter) بوصفه مصدراً للبيانات (زيمير وبروفيريس [Zimmer and Proferes]، 2014، ص. 256). قد يتمتّع الباحثون بحرّية كبيرة، ولكن ثمّة توجيه رسمي قليل حول كيفية استخدام مصدر البيانات الجديد هذا بشكلٍ أخلاقي.

في حين لا تستطيع وزارة الدفاع الأمريكية (DoD) أن تعكس ببساطة العالم الأكاديمي، قد تظهر فائدة من الاعتماد على عملٍ مماثلٍ أُجرِي في الوسط البحثي الأكاديمي. وبما يشبه إلى حدّ كبير الأسئلة العسكرية حول الباب 10 مقابل الباب 50، ترتكز النقاشات الأكاديمية حول أخلاقيات البحث على الإنترنت إلى السياق والنيّة: "يعتمد تشكيل مفاهيم لأخلاقيات البحث على الإنترنت على مناظير تأديبية" (بوشنان وزيمر [Buchanan and Zimmer]، 2016). ومثل الجيش، يحاول الوسط الأكاديمي التعامل مع التعقيد الكامن في وسائل التواصل الاجتماعي. لدى التخطيط لعمليات المعلومات (IO) ودمجها، يُنظر إلى "وسائل التواصل الاجتماعي" بوصفها موقعاً وطريقةً لتبادل الرسائل، ومصدراً للبيانات ومجموعةً من الأساليب التحليلية؛ بالمثل، يُعتبر البحث على الإنترنت أسلوباً وموقعاً للبحث على حدّ سواء، ويقترن بتنوّع واسع النطاق بحيث لا يمكن اعتباره أمراً واحداً (اللجنة الاستشارية لحماية الموارد البشرية التابعة للوزير [Secretary's Advisory Committee on Human Resource Protections]، 2013، ص. 2).

أخلاقيات الخصوصيّة

في ما يتجاوز الامتثال القانوني، ثمّة بعض الانتقادات المحتملة المرتكزة إلى الأخلاقيات لجهود تحليل وسائل التواصل الاجتماعي التي تبذلها وزارة الدفاع الأمريكية (DoD). قد ترتكز هذه الانتقادات إلى التمييزات بين ما يُعتبر عاماً وما يُعتبر خاصاً. فعلى سبيل المثال، حصل انتقاد عام لبرنامج المراقبة بريزم التابع لوكالة الأمن القومي (NSA's PRISM program) باعتبار أنّه ينتهك التوقّعات من حيث الخصوصيّة. في حين تنطوي تلك الحالة على نشاطات داخلية لن تنخرط فيها وزارة الدفاع الأمريكية، قد تمتدّ التمييزات الثقافية الأمريكية بين البيانات الخاصة والبيانات العامة إلى جمع البيانات والعمليات غير الأمريكية.

يواجه علماء الأبحاث المدنيون مخاوف مماثلة بشأن البيانات العامة والخاصة.

ويتمثّل الموقف الناشئ بأنّه يمكن التفكير في الفضاءات الرقمية بشكلٍ متماثلٍ على أنّها تعكس سلوك العالم الحقيقي العام أو الخاص:

> يمكن تشبيه الفضاءات العامة بمراقبة السلوك في العامة. في الحالات حيث تذكر شروط الخدمة بوضوح أن المحتوى سيُتاح للعامة، لن تكون الموافقة ضرورية لإجراء بحثٍ حول المعلومات المُتاحة للعامة. لا يزال على الباحثين المحافظة على مدونات أخلاقياتهم وحماية خصوصية الأشخاص موضوع بحثهم. (مورفي وآخرون [Murphy et al.]، 2014، ص. 6).

قد تشير مقاربة تتبع نهجاً منطقياً للتمييز بين الطبيعة العامة أو الخاصة لمصدر بيانات، مثل تويتر (Twitter)، إلى شروط الخدمة، التي توضّح أنّ مدخلات المُستَخدِم ستكون عامّة. تتعارض واجهة برمجة التطبيقات (API) العامة الأصلية الخاصة بتويتر والبيع العام لبيانات تويتر من خلال بائعين من أطراف ثالثة، مع منصات وسائل التواصل الاجتماعي التي تتمتّع بإعدادات الخصوصية وشبكات محدّدة المُستخدِم بالنسبة للتبادل: "يتم ضمان نشر رسائل تويتر البارزة للعامة على الإنترنت عموماً، أقلّه تقنياً، وتؤدي بالتالي أرشفتها في سياق نشاطات البحث إلى إشكاليات أقلّ بكثير" (زيمير وبروفيريس [Zimmer and Proferes]، 2014، ص. 13).

في حين نلاحظ أنّه قد يتم طرح أسئلة حول مدى فهم عامّة الجمهور لمفاهيم الخصوصية وعمليات الإفصاح عن المعلومات، اعتمدت وزارة الدفاع الأمريكية مقاربة تتبع نهجاً منطقياً وتتسق مع مواقف الباحثين المدنيين والتي تتعامل مع المعلومات المتوفرة على نطاقٍ واسعٍ على أنّها "عامّة" (كتيّب وزارة الدفاع الأمريكية 01.5240 [U.S. Department of Defense Manual 5240.01، 2016، ص. 53).

الاعتبارات المرتبطة بالبيانات والتكنولوجيا

يتوجب على وزارة الدفاع الأمريكية (DoD) أن تراجع أيضاً القضايا المحيطة بالاستحواذ على التكنولوجيا والبيانات التحليلية الخاصة بوسائل التواصل الاجتماعي. لا تتعلق هذه القضايا بالتكاليف فحسب، وإنّما أيضاً بالفعالية والمفاضلات بين استراتيجيات الاستحواذ المختلفة. فعلى سبيل المثال، قد يكون اللجوء إلى البائعين التجاريين أمراً جذاباً. من الممكن أن يكون هؤلاء البائعون قد طوّروا تكنولوجيا متطوّرة في أسواق تنافسية، بما في ذلك الحلول التي يمكن شراؤها وتكون جاهزة ويمكن استخدامها بسرعة. على الرغم من ذلك، قد ترد عدم تطابقات مهمّة في السياق والغرض بين الحاجات التشغيلية التجارية

والعسكرية. فعلى سبيل المثال، يُعتبر تحليل المشاعر لإدارة العلامة الفارقة مختلفاً جداً عن تحليل المشاعر للحصول على رؤية حول استراتيجيات الحُجج العامة.

في مقابلاتنا مع الخبراء في الموضوع في القطاعين التجاري والعسكري، وجدنا أربعة مخاوف رئيسية:

- **تكاليف الاستحواذ على البيانات والتكنولوجيا**. ترتفع تكاليف الاستحواذ على البيانات؛ ويتجسّد مثلٌ جيد حول ذلك بقرار تويتر (Twitter) القاضي بقطع إمكانية وصول الموزّعين من أطراف ثالثة إلى البيانات وارتفاعات أسعار البيانات الناتجة عن ذلك. بغضّ النظر عن أي تغييرات في الكلفة، تشير الزيادة الهائلة في حجم بيانات وسائل التواصل الاجتماعي ذات الصلة، بما في ذلك الانفجار المحتمل للبيانات من إنترنت الأشياء (Internet of Things) إلى تيارٍ صاعدٍ من تكاليف الاستحواذ على البيانات. ثمّة أيضاً تكاليف كبيرة في الاستحواذ على التكنولوجيا، والتي ستتأثّر إلى حدٍّ كبيرٍ باستراتيجية الاستحواذ المُختارة (مثلاً، التعاقد المستمر مقابل الاستحواذ من مصدر مفتوح).
- **مكانة القدرة البشرية في تحليلات بيانات وسائل التواصل الاجتماعي**. أشار بعض الذين قمنا بمقابلتهم إلى نطاق وقوّة الأنظمة التحليلية الممكننة بشكلٍ كاملٍ بوصفها المستقبل الأكثر وعداً. وأشار آخرون إلى الحاجة إلى معنى ومنطق بشريين في التحليل، بدلاً من مقاربةٍ تحليليةٍ بضغطة زرّ.
- **تحليل التوسّع**. سلّط الخبراء الضوء على الحاجة إلى حلول لـ"فرز البيانات" وتوفير تدفقات من المعلومات يمكن إدارتها للمحللين البشريين. تدعو الحاجة إلى تكنولوجيا تستطيع إعداد البيانات الموحّدة وغير الموحّدة للمنطق البشري.
- **المعايير والتبادل**. تتطلّب وزارة الدفاع الأمريكية (DoD) صورة تشغيل مشتركة للتحليل الفعّال لوسائل التواصل الاجتماعي. في غياب حلّ أو معيار على مستوى المؤسسة، مع هندسة بيانات مشتركة، لا تتوفر لكيانات عمليات المعلومات (IO) أي طريقة لتبادل البيانات الخام أو نتائج التحليل أو التجسيدات المرئية. وبالإضافة إلى ذلك، وفي غياب مثل هذا المعيار، لا تتوفر أي طريقة منهجية لاختبار التكنولوجيا أو الأساليب الجديدة مقابل مجموعات البيانات القائمة.

الاعتبارات المرتبطة بالتدريب

تتمثّل قضية أخرى تواجه وزارة الدفاع الأمريكية (DoD) بالتدريب. في هذا المجال الجديد، ما هي المهارات والمعرفة المطلوبة من أجل إنتاج قدرة تحليلية صلبة وفعالة

فيما يتعلق بوسائل التواصل الاجتماعي وإدامتها؟ تملك وزارة الدفاع الأمريكية حالياً إمكانية الوصول إلى التدريب الأساسي والتعاقدي عبْر الاختصاصات الإلكترونية، بما فيها استخراج البيانات. يشمل بعض هذا التدريب عناصر من تحليل وسائل التواصل الاجتماعي، بما في ذلك قابلية تطبيقه على عمليات المعلومات (IO) والعمليات العسكرية. على الرغم من ذلك، أشار الخبراء الذين قمنا بمقابلتهم إلى وجود نقصٍ في التدريب المُصمم خصيصاً لمساعدة المحللين على فهم بيانات وسائل التواصل الاجتماعي. وبحسب ما عَبَّرَ عنه أحد الذين تمت مقابلتهم، "في الوقت الحالي، كل ما يمكننا فهمه هو 'عِلم الأزرار'؛ اضغط على زر، تحصل على موزة" (مقابلة مع خبيرٍ متخصّص في الموضوع، 29 أغسطس/آب 2016). وتمثّلت قضية أخرى ظهرت بالحاجة إلى التدريب على المراقبة في مجال الامتثال القانوني. وبالنظر إلى دعوة الكونغرس لوضع سياسات خاصة بوزارة الدفاع الأمريكية حول استخدام وسائل التواصل الاجتماعي والمعلومات الأخرى المُتاحة للعامة، ستدعو الحاجة إلى تدريبٍ رسمي في مجال المراقبة والامتثال.

التوصيات

بالاعتماد على مراجعتنا للدراسات السابقة المتوفرة حول تحليلات بيانات وسائل التواصل الاجتماعي في سياق عمليات المعلومات (IO) وعلى مقابلاتنا مع خبراء متخصصين في الموضوع، نقدّم مجموعة من التوصيات حول كيفيّة تمكّن وزارة الدفاع الأمريكية (DoD) من بناء قدرةٍ على تحليل وسائل التواصل الاجتماعي دعماً لعمليات المعلومات ونشرها بطريقةٍ أكثر فعالية وإنتاجية. تغطّي هذه التوصيات قضايا غير تقنيّة (مثلاً، المخاوف القانونية والأخلاقية)، وقضايا التنفيذ العقائدية والمؤسساتية، وقضايا تقنية بشأن كيفية تحليل بيانات وسائل التوصال الاجتماعي وبناء قدرة تقنية بشكلٍ مفيدٍ.

تطوير سياسات ولغة خاصّة بوزارة الدفاع الأمريكية (DoD) لتحليل وسائل التواصل الاجتماعي

التوصيات القانونية

لدى وزارة الدفاع الأمريكية (DoD) حاجة تشغيلية مشروعة وملحّة لجمع بيانات وسائل التواصل الاجتماعي وتحليلها. يتمثّل تحدٍّ كبيرٍ بأنّه تمّ تطبيق أطر العمل القانونية المُطوَّرَة للعمليات العسكرية التقليدية والإشراف على الاستخبارات/العمليات السريّة المنصوص عليها في الباب 50 على حدّ سواء على عمليات المعلومات (IO) الخاصة بالجيش الأمريكي. وكما سبق وفصّلنا، يتم نقل أطر العمل القانونية هذه بشكلٍ ضعيف، وتقترن بفجوات كبيرة، وبغموض وبعدم تطابقات. تتمثّل خطوة أولى ضروريّة في استيفاء المتطلّبات القانونية الأمريكية بخصوص جمع بيانات وسائل التواصل الاجتماعي وتحليلها — مع أيضاً تلبية حاجات الأمن القومي بفعالية — لتبيان الفَرْق الهادف بين عمليات المعلومات العسكرية بموجب الباب 10 من قانون الولايات المتحدة ومراقبة الاستخبارات الأجنبية التي يتم إجراؤها بموجب الباب 50، والأمر التنفيذي رقم 12333 وقانون مراقبة الاستخبارات الأجنبية (Foreign Intelligence Surveillance Act). ويجب أن يشمل

هذا التبيان ما يلي:

- توضيح صلة سلطة القيادة بالعمليات ونيّتها منها، بدلاً من أساليب البيانات أو مصدرها، من خلال التمييز بين العمليات المنصوص عليها في الباب 10 وتلك المنصوص عليها في الباب 50. يختلف استخدام وسائل التواصل الاجتماعي من أجل تحديد عُقدة شبكة رئيسية للاستهداف بقوةٍ قاتلةٍ في سياق عملية منصوص عليها في الباب 50 تديرها وكالة استخبارات اختلافاً قاطعاً عن استخدام الأسلوب نفسه والبيانات نفسها من أجل تحديد عُقدة شبكة دعماً لجهد عمليات دعم المعلومات العسكرية (MISO).
- التمييز بين "استخدام القوّة" في العمليات التقليدية واستخدام القدرات المرتبطة بالمعلومات (IRCs) غير الحركيّة، مثل عمليات دعم المعلومات العسكرية (MISO) أو الشؤون العامة. يعكس القانون الحالي القِيَم الأمريكية من خلال التمييز بين المقاتلين وغير المقاتلين في استخدام القوّة، ولكنّه يتعثّر مثلاً في حال سوء تمييز جهود مكافحة الدعاية التي تهدف إلى الحدّ من صراع بوصفه "استخدام للقوة".
- معالجة تعقيد الطبقات المتداخلة من القانون والسياسات الداخلية التي قد تنطبق على عمليات المعلومات (IO) والقدرات المرتبطة بالمعلومات (IRCs)، بالإضافة إلى كيفية معالجة أوجه الاختلاف بين القوانين الواجبة التطبيق في الولايات المتّحدة وفي أممٍ أخرى.
- إنارة السياسات والعقيدة بمبادئ واضحة تهدف إلى حماية الأشخاص الأمريكيين بشكلٍ معقولٍ من جمع البيانات، والتمييز بين العمليات الموجّهة نحو الأشخاص الأمريكيين والعمليات التي قد تجمع بشكل عرضي بيانات حول أشخاص أمريكيين كمنتجٍ ثانويٍّ للمُتَناول العالمي لأنظمة التواصل الحديثة ووسائل التواصل الاجتماعي.

تطوير اللغة الخاصة بالباب 10 لتحليل وسائل التواصل الاجتماعي

كانت وزارة الدفاع الأمريكية (DoD) تستخدم اللغة وإطار العمل المفاهيمي الخاصّين بالكيانات المنصوص عليها في الباب 50، ويعزّز استخدام كلمات مثل **الجمع** و**الاحتفاظ** إطار عمل استخباراتي/سريّ، على عكس إطار عمل للعمليات العسكرية/عمليات المعلومات (IO). يتوجّب على وزارة الدفاع الأمريكية، لدى تطوير سياسات تعكس حاجاتها، أن تضع مصطلحات متخصصة دقيقة ومميّزة للاستحواذ على بيانات وسائل التواصل الاجتماعي وتخزينها وتحليلها ويتوجب عليها دمج هذه اللغة في مذكرات العقيدة والسياسات. قد تشمل الأمثلة إلغاء المصطلح **جمع** لصالح المصطلح **استحواذ**، أو إلغاء المصطلح **احتفاظ** لصالح المصطلح **تخزين**.

التوصيات الأخلاقيّة

بالإضافة إلى ضمان الامتثال القانوني في عمليات المعلومات (IO)، يجب أن تأخذ قدرةٌ معقولةٌ ومستدامة على تحليل وسائل التواصل الاجتماعي تلبّي حاجات الأمن القومي بعين الاعتبار أيضاً المعايير الأخلاقية في الثقافة الأمريكية. تشمل توصياتنا للاعتبارات الأخلاقيّة خيارات العمليات، والممارسات الفضلى المُقترحة، وتوصيات خاصّة بشأن ضوابط الخصوصيّة.

المبادئ مقابل المدوّنات

بوصفها توصية بشأن عملية شاملة، نرى أنّه يتوجب على وزارة الدفاع الأمركية (DoD) صياغة **مبادئ سلوك** مرنة ونشرها، بدلاً من مجموعاتٍ من القواعد الثابتة والراسخة. ويُعتبر هذا الأمر مهماً بشكلٍ خاص بالنظر إلى الطبيعة السريعة التطوّر لتكنولوجيات وسائل التواصل الاجتماعي واتجاهاتها. سيتيح ذلك أيضاً لقادة الجيش الأمريكي تفعيل السلوك الأخلاقي بطرقٍ مُحدَّدَة السياق محلياً، ما يؤدي حثياً إلى نتائج أخلاقية لدرجة أكبر مما قد يكون ممكناً بموجب مجموعات القواعد المدّوَنة (ماركهام وبوشنان [Markham and Buchanan]، 2012، ص. 5).

الممارسات الفضلى لجمع البيانات

يتوجّب على وزارة الدفاع الأمريكية (DoD) تطوير مجموعة من الممارسات الفضلى المرتكزة إلى المعايير لجمع بيانات وسائل التواصل الاجتماعي والتي تعكس القِيَم الأمريكية ولا تعيق إنجاز المهمّة. ويجب أن تشمل مجموعة عملية من الممارسات العناصر التالية (بارتليت ورينولدز [Bartelett and Reynolds]، 2015):

- حيث أمكن، الإعلان عن أهداف البحث وأساليبه وجعلها واضحةً مع حماية تقنيات التجسس وإجراءاته والعمليات الجارية.
- تأسيس مبدأ "تناسب" مطوّر بشكلٍ جيّد وصريح، يحقّق التوازن بين التدخّل الناتج عن جمع البيانات وحاجات الأمن القومي المعقولة.
- اتّخاذ إجراءات احتياطيّة معقولة من أجل ضمان أنّ أساليب تخزين مجموعات بيانات وسائل التواصل الاجتماعي وتوزيعها — حتّى تلك المجهولة المصدر — تحمي الأشخاص من تحديد هويتهم من خلال الإحالة المرجعية أو الرصد التثليثي.
- تطوير ونشر معايير لقياس الخطر الذي تطرحه جهود الجمع بالنسبة للاستخدام الحرّ والمفتوح لوسائل التواصل الاجتماعي والإنترنت مقابل منافع الأمن القومي. ويجب أن يشمل هذا المعيار أيضاً تقييماً لتبرير استخدام الأموال العامّة لجهد جمعٍ معيّن.
- تطوير ونشر معيار بشأن التوقّع المعقول للخصوصية فيما يتعلق بجمع وزارة

الدفاع الأمريكية (DoD) لبيانات وسائل التواصل الاجتماعي، والذي يحقق التوازن بين حاجات الأمن القومي وتوقّعات العامّة بشأن الشفافية (بارتليت ورينولدز [Bartelett and Reynolds]، 2015).

التوصيات للتنفيذ والدمج

عالج تحليلنا **كيفية** التمكّن من دمج تحليلات بيانات وسائل التواصل الاجتماعي بفعالية في عمليات معلومات وزارة الدفاع الأمريكية (DoD IO)، بالإضافة إلى **طرق** تنفيذ هذه المقاربات. وبالتالي، نقدّم التوصيات التالية بخصوص تنفيذ وزارة الدفاع الأمريكية لاستراتيجية تحليلية خاصة بوسائل التواصل الاجتماعي.[1]

إطار عمل يرتكز إلى القدرات المرتبطة بالمعلومات (IRCs) للتنفيذ

تُعتبر مقاربات البيانات الضخمة لعمليات المعلومات (IO)، بما فيها تحليل وسائل التواصل الاجتماعي، في مرحلتها الناشئة. وتشكّل حداثة مفاهيم وسائل التواصل الاجتماعي، ومصطلحاتها وممارساتها عائقاً في وجه الاعتماد والتنفيذ. سيساعد الربط بين المعلومات الجديدة والمعلومات المعروفة وزارة الدفاع الأمريكية (DoD) في دمج هذه الأساليب والأدوات الجديدة بطريقةٍ أفضل. قدّم الفصل الثاني إطار عمل مبدئياً يرتكز إلى القدرات المرتبطة بالمعلومات (IRCs) لفهم تحليل وسائل التواصل الاجتماعي وتنفيذه كنقطة انطلاق لدمجه في عقيدة عمليات المعلومات وممارستها.

جهد تحليل وسائل التواصل الاجتماعي على مستوى المؤسسة

تُعتبر الجهود الحالية لبناء قدرةٍ على تحليل وسائل التواصل الاجتماعي داخل وزارة الدفاع الأمريكية (DoD) محلية وغير منسّقة عَبْر المستويات وبينها. يتم استخدام المقاربات التحليلية الخاصة بوسائل التواصل الاجتماعي من أجل حلّ مشاكل على مستوى قيادات المقاتلين وضمن الأجهزة على مستوى القيادة. قد تؤدي هذه المجموعة الموزّعة من الجهود إلى الابتكار من خلال توفير عددٍ من المواقع الحاضنة، ولكن لنقص الوحدة سلبيات متعددة:

- إنّه يحول دون احتمال تحقيق وفورات في التكاليف من خلال جهدٍ على مستوى

[1] يتوجّب على وزارة الدفاع الأمريكية (DoD) أن تنظر بتأنٍ في كيفية بناء القدرة بالطريقة الأفضل من منظور إدارة الكادر. لا يقدّم هذا التقرير توصيات محددة بشأن مزايا وعيوب تطوير قدرةٍ من قِبَل أعضاء التدريب مقابل توظيف موظّفي الحكومة أو اللجوء إلى خدمات المقاولين، ولكن لا تزال القضية قائمة، ويجب معالجتها.

المؤسسة. ويُعتبر هذا الموضوع مهماً بشكلٍ خاصٍ من حيث تكاليف الاستحواذ على البيانات، ولكن قد يتم أيضاً تحقيق وفورات في التكاليف للاستحواذ على البيانات والتدريب على حدٍ سواء من جهدٍ منسّقٍ على نطاق وزارة الدفاع الأمريكية (DoD).

- يزيد من خطر مسارات نقل المعلومات.

بالتالي، إنّنا نوصي بأن تنظر وزراة الدفاع الأمريكية في المنافع والمخاطر المرتبطة بجهد تحليل وسائل التواصل الاجتماعي على مستوى المشروع.

التوصيات التقنية

الاستحواذ على التكنولوجيا

تُحبّذ مراجعتنا للمقاربات التحليلية الخاصة بوسائل التواصل الاجتماعي التكنولوجيات والأساليب القائمة المفتوحة المصدر. في حين نقرّ بأنّ الحلول من القطاع التجاري مطوّرة من الناحية التكنولوجية وتقترن بقدرةٍ كامنةٍ كبيرة، ثمّة أيضاً سلبيات محتملة من حيث كلفة تحويل هذه الحلول وقابلية تطبيقها. من أجل المضي قُدُماً في تحليل وسائل التواصل الاجتماعي، يتوجب على وزارة الدفاع الأمريكية (DoD) أن تقارن تكاليف ومنافع استخدام الحلول المفتوحة المصادر مقابل الحلول التجارية. وعلى وجه الخصوص، يتوجب عليها أن تأخذ المفاضلات التالية بعين الاعتبار:

- لدى البائعين التجاريين مصلحة مكتسبة للمحافظة على سريّة التقدّمات وحصرية ملكيتها، ولذلك فهُم يميلون إلى إنتاج حلول "الصندوق الأسود" التي تُظهر النتائج فحسب (وليس العمليات) للمُستَخدِمين. قد تكون حلول الصندوق الأسود مطوّرة جداً، ولكن ما لم ينظر أحدٌ في المؤسسة على ما لا يمكن رؤيته ويرى العملية، بما في ذلك الافتراضات المُضمّنة والمفاضلات والقرارات بالوكالة، لا يمكن التأكيد على صحّة النتائج.
- قد تعمل استراتيجيات التسييل الخاصة بالكيانات التجارية لما هو ضدّ مصلحة الحكومة. فعلى سبيل المثال، قد يكون التفاوض على عقدٍ جارٍ من أجل توفير الخدمات استخداماً غير فعّال للأموال العامّة بالمقارنة مع مقاربة "علّمني الصيد" التي توفّر لمحلّلي وزارة الدفاع الأمريكية (DoD) أدوات وتدفقات أعمال قابلة للاستخدام.
- لا يمكن نقل التكنولوجيات أو الحلول جميعها إلى سياقات وزارة الدفاع الأمريكية الوظيفية ووقائعها.

التدريب واكتساب المهارات

إنّ التدريب الحالي في مجال الاختصاصات الإلكترونية داخل وزارة الدفاع الأمريكية (DoD) غير كافٍ لدعم قدرةٍ صلبةٍ على تحليل وسائل التواصل الاجتماعي. من أجل معالجة هذا النقص، نقدّم التوصيات التالية:

- بالنظر إلى دعوات الكونغرس لوضع سياسات محددة حول استخدام وسائل التواصل الاجتماعي وغيرها من المعلومات المُتاحة للعامّة، ستدعو الحاجة إلى تدريبٍ رسميٍّ داخل وزارة الدفاع الأمريكية (DoD) حول المراقبة والامتثال.
- إلى الحدّ الذي تختار فيه وزارة الدفاع الأمريكية (DoD) بناء قدرتها على تحليل وسائل التواصل الاجتماعي باستخدام الكادر العسكري، يجب أن يتجاوز التدريب "عِلم الأزرار" لتعليم المحلّلين كيفية فهم بيانات وسائل التواصل الاجتماعي.

يقدّم الجدول رقم 5.1 ملخّصاً للخطوات القادمة لوزارة الدفاع الأمريكيّة (DoD) وهي تُواصِل استكشاف العوامل المعنية بتطوير قدرةٍ على تحليل وسائل التواصل الاجتماعي وتنفيذها وتعالج التحدّيات القانونية وتلك المرتبطة بالسياسات لدى القيام بذلك.

الجدول رقم 5.1
خارطة طريق للاستفادة من تحليل وسائل التواصل الاجتماعي لحملات عمليات معلومات وزارة الدفاع الأمريكية (DoD IO)

التدبير	النتيجة
إجراء مراجعة قانونية على مستوى وزارة الدفاع الأمريكية (DoD) لدعم عمليات المعلومات (IO) من قِبَل المنظّمات المنصوص عليها في الباب 10.	إجراء تحديث على المنشور المشترك 3-13 (JP 3-13)، عمليات المعلومات (IO)، يقدّم الإرشاد القانوني والمحدوديات للقادة ومخططي عمليات المعلومات، بما في ذلك اللغة الخاصة بالباب 10 لاستخدام البيانات المتمحورة حول عمليات المعلومات
صياغة مبادئ توجيهية واضحة للاستحواذ على البيانات المتمحورة حول عمليات المعلومات (IO) وتخزينها واستخدامها ضمن وزارة الدفاع الأمريكية (DoD). يجب إناره هذه المبادئ التوجيهية من قِبَل جهودٍ مماثلةٍ من القادة الأكاديميين والصناعيين.	مذكرة سياسات لوزارة الدفاع الأمريكية (DoD) تجعل المبادئ التوجيهية الخاصة بالسياسات واضحةً وتحدد المعايير لقياس المخاطر والمنافع للأمن القومي
تحليل نقاط القوة ونقاط الضعف لقدرة وزارة الدفاع الأمريكية (DoD) على تحليل وسائل التواصل الاجتماعي على مستوى المؤسسة، وفرص تطويرها وتكاليفه (بما في ذلك التدريب)، وخصائص التهديدات التي تواجهها.	قرار صريح على مستوى السياسات للاختيار بين إما جهود الخدمة المتخصصة/قيادة المقاتلين المحدّدة لإجراء الدراسات التحليلية الخاصة بوسائل التواصل الاجتماعي أو جهد على مستوى المؤسسة عَبْر وزارة الدفاع (DoD)
التكليف بإجراء مراجعةٍ مستقلّة لتقديم المشورة للحكومة الأمريكية بشأن الاستحواذ على التكنولوجيا، مع التركيز على منافع ومفاضلات المصدر المفتوح مقابل استراتيجيات الاستحواذ التجاري.	مذكرة لسياسات وزارة الدفاع الأمريكية (DoD) تحدد المعايير للاستحواذ على التكنولوجيا التجارية دعماً لتحليل وسائل التواصل الاجتماعي

المراجع

Abbasi, Mohammad-Ali, Shamanth Kumar, Jose Augusto Andrade Filho, and Huan Liu, "Lessons Learned in Using Social Media for Disaster Relief—ASU Crisis Response Game," *Lecture Notes in Computer Science*, Vol. 7227, New York: Springer, 2012, pp. 282–289.

Al-Malki, Amal, David Kaufer, Suguru Ishizaki, and Kira Dreher, *Arab Women in Arab News: Old Stereotypes and New Media*, London: Bloomsbury, 2012.

Baker, Paul, Costas Gabrielatos, Majid Khosravinik, Michał Krzyżanowski, Tony McEnery, and Ruth Wodak, "A Useful Methodological Synergy? Combining Critical Discourse Analysis and Corpus Linguistics to Examine Discourses of Refugees and Asylum Seekers in the UK Press," *Discourse and Society*, Vol. 19, No. 3, May 2008, pp. 273–306.

Bartlett, Jamie, and Louis Reynolds, *The State of the Art 2015: A Literature Review of Social Media Intelligence Capabilities for Counter-Terrorism*, London: Demos, 2015.

Berger, J. M., and Jonathon Morgan, *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter*, Washington, D.C.: Brookings Institution, March 2015. As of March 16, 2017: https://www.brookings.edu/research/the-isis-twitter-census-defining-and-describing-the-population-of-isis-supporters-on-twitter

Bodine-Baron, Elizabeth, Todd C. Helmus, Madeline Magnuson, and Zev Winkelman, *Examining ISIS Support and Opposition Networks on Twitter*, Santa Monica, Calif.: RAND Corporation, RR-1328-RC, 2016. As of March 16, 2017: http://www.rand.org/pubs/research_reports/RR1328.html

Bodine-Baron, Elizabeth, William Marcellino, Doug Yeung, and Zev Winkelman, "Social Media Analysis Across Language and Geography," presentation at the conference Social Media and Online Behavior: Language and Culture Considerations and Challenges for the Intelligence Community, College Park, Md., June 11, 2015.

Boehnert, John M., *Influencing Tomorrow: A Study of Emerging Influence Techniques and Their Relevance to United States Information Operations*, thesis, Fort Leavenworth, Kan.: U.S. Army Command and General Staff College, 2015.

Buchanan, Elizabeth A., and Michael Zimmer, "Internet Ethics Research," *Stanford Encyclopedia of Philosophy*, revised August 24, 2016. As of March 16, 2017:
https://plato.stanford.edu/entries/ethics-internet-research/

Chesney, Robert, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," *Journal of National Security Law and Policy*, Vol. 5, No. 2, 2012, pp. 539–629.

Correa, Denzil, and Ashish Sureka, "Solutions to Detect and Analyze Online Radicalization: A Survey," *IITD PhD Comprehensive Report*, Vol. 5, No. N, January 2013. As of March 16, 2017:
https://arxiv.org/pdf/1301.4916v1.pdf

Dauber, Cori E., *YouTube War: Fighting in a World of Cameras on Every Cell Phone and Photoshop on Every Computer*, Carlisle Barracks, Pa.: Strategic Studies Institute, U.S. Army War College, November 2009. As of March 16, 2017:
http://www.au.af.mil/au/awc/awcgate/ssi/youtubewar_dauber.pdf

DoD—*See* U.S. Department of Defense.

Drapeau, Mark, and Linton Wells II, *Social Software and National Security: An Initial Net Assessment*, Monterey, Calif.: Center for Technology and National Security Policy, National Defense University, April 2009.

Duncan, Matthew, *Future Casting Influence Capability in Online Social Networks*, Toronto, Ont.: Defence Research and Development Canada, 2015.

Elstad, Peter L., *Overcoming Information Operations Legal Limitations in Support of Domestic Operations*, thesis, Fort Leavenworth, Kan.: U.S. Army Command and Staff College, 2008.

Everstine, Brian, "Carlisle: Air Force Intel Uses ISIS 'Moron's' Social Media Posts to Target Airstrikes," *Air Force Times*, June 4, 2015. As of March 16, 2017:
http://www.airforcetimes.com/story/military/tech/2015/06/04/air-force-isis-social-media-target/28473723

Gendron, Jr., Gerald R., Herminio Blas-Irizarry, and Jesse W. Boggs, *Next-Generation Strategic Communication: Building Influence Through Online Social Networking*, thesis, Norfolk, Va.: Joint and Combined Warfighting School, Joint Forces Staff College, June 2009.

Gilinsky, Jaron, "How Social Media War Was Waged in Gaza-Israel Conflict," MediaShift, February 13, 2009. As of March 16, 2017:
http://mediashift.org/2009/02/how-social-media-war-was-waged-in-gaza-israel-conflict044

Goolsby, Rebecca, *On Cybersecurity, Crowdsourcing, and Social Cyber-Attack*, Washington, D.C.: Wilson Center, 2013. As of March 16, 2017: https://www.wilsoncenter.org/sites/default/files/127219170-On-Cybersecurity-Crowdsourcing-Cyber-Attack-Commons-Lab-Policy-Memo-Series-Vol-1.pdf

Hollis, Duncan B., "New Tools, New Rules: International Law and Information Operations," in G. J. David, Jr., and T. R. McKeldin, eds., *Ideas as Weapons: Influence and Perception in Modern Warfare*, Washington, D.C.: Potomac Books, 2009, pp. 59–72.

Joint Publication 3-13, *Information Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, incorporating change 1, November 20, 2014.

JP—*See* Joint Publication.

Jurich, Jon P., "Cyberwar and Customary International Law: The Potential of a Bottom-Up Approach to an International Law of Information Operations," *Chicago Journal of International Law*, Vol. 9, No. 1, Summer 2008, pp. 275–295.

Kase, Sue E., Elizabeth K. Bowman, Tanvir Al Amin, and Tarek Abdelzaher, *Exploiting Social Media for Army Operations: Syrian Civil War Use Case*, Aberdeen Proving Ground, Md.: Army Research Laboratory, July 2014.

Katz, Yaakov, "Facebook Details Cancel IDF Raid," *Jerusalem Post*, March 4, 2010. As of March 16, 2017: http://www.jpost.com/Home/Article.aspx?id=170156

Keller, Rebecca A., *Influence Operations and the Internet: A 21st Century Issue*, Maxwell Air Force Base, Ala.: Air War College, Air University, Paper No. 52, February 17, 2010. As of March 16, 2017: http://www.au.af.mil/au/awc/awcgate/maxwell/mp52.pdf

Khazan, Olga, "Russia's Online-Comment Propaganda Army," *The Atlantic*, October 9, 2013. As of March 16, 2017: http://www.theatlantic.com/international/archive/2013/10/russias-online-comment-propaganda-army/280432

Kumar, Shamanth, Geoffrey Barbier, Mohammad Ali Abbasi, and Huan Liu, "TweetTracker: An Analysis Tool for Humanitarian and Disaster Relief," *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media*, Palo Alto, Calif.: Association for the Advancement of Artificial Intelligence, 2011, pp. 661–662.

Laje, Diego, "#Pirate? Tracking Modern Buccaneers Through Twitter," CNN, March 15, 2012. As of March 16, 2017: http://www.cnn.com/2012/03/15/business/somalia-piracy-twitter

Levin, Megan, "Social Media and Intelligence," presentation, Embry-Riddle Aeronautical University, Prescott, Ariz., Spring 2015. As of March 16, 2017: http://commons.erau.edu/pr-honors-csi/1/?utm_source=commons.erau.edu%2Fpr-honors-csi%2F1&utm_medium=PDF&utm_campaign=PDFCoverPages

Marcellino, William M., "Revisioning Strategic Communication Through Rhetoric and Discourse Analysis," *Joint Force Quarterly*, No. 76, First Quarter 2015, pp. 52–57. As of March 16, 2017: http://ndupress.ndu.edu/Media/News/News-Article-View/Article/577589/jfq-76-revisioning-strategic-communication-through-rhetoric-and-discourse-analy

Marcellino, William M., Kim Cragin, Joshua Mendelsohn, Andrew Cady, Madeline Magnuson, and Kathleen Reedy, "Measuring the Popular Resonance of Daesh's Propaganda," *Journal of Strategic Security*, Vol. 10, No. 1, 2016, pp. 32–52.

Markham, Annete, and Elizabeth Buchanan, *Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee (Version 2.0)*, Chicago, Ill.: Association of Internet Researchers, 2012. As of March 16, 2017: https://aoir.org/reports/ethics2.pdf

Murphy, Joe, Michael W. Link, Jennifer Hunter Childs, Casey Langer Tesfaye, Elizabeth Dean, Michael Stern, Josh Pasek, Jon Cohen, Mario Callegaro, and Paul Harwood, *Social Media in Public Opinion Research: Report of the AAPOR Task Force on Emerging Technologies in Public Opinion Research*, Oakbrook Terrace, Ill.: American Association for Public Opinion Research, 2014. As of March 16, 2017: https://www.aapor.org/AAPOR_Main/media/MainSiteFiles/AAPOR_Social_Media_Report_FNL.pdf

Nelson, Anne, "How Mapping, SMS Platforms Saved Lives in Haiti Earthquake," MediaShift, January 11, 2011. As of March 16, 2017: http://mediashift.org/2011/01/how-mapping-sms-platforms-saved-lives-in-haiti-earthquake011

Omand, David, Jamie Bartlett, and Carl Miller, "Introducing Social Media Intelligence (SOCMINT)," *Intelligence and National Security*, Vol. 27, No. 6, 2012, pp. 801–823.

Opperman, Duane A., *Information Operations and Public Affairs: A Union of Influence*, Carlisle Barracks, Pa.: U.S. Army War College, March 2012.

Oreskovic, Alexei, "Here's Another Area Where Twitter Appears to Have Stalled: Tweets per Day," *Business Insider*, June 15, 2015. As of March 16, 2017: http://www.businessinsider.com/twitter-tweets-per-day-appears-to-have-stalled-2015-6

Phillips, Kenneth N., and Aaron Pickett, "Embedded with Facebook: DoD Faces Risks from Social Media," *Crosstalk Magazine*, May–June 2011, pp. 25–29.

Schoen, Rudy, *Social Media: Valuable Tools in Today's Operational Environment*, Newport, R.I.: Joint Military Operations Department, 2011.

Scott, Mike, Wordsmith Tools, software, version 7.0, Lexical Analysis Software and Oxford University Press, 2016.

———, "Mapping Key Words to Problem and Solution," in Mike Scott and Geoff Thompson, eds., *Patterns of Text: In Honour of Michael Hoey*, Amsterdam, The Netherlands: John Benjamins Publishing Co., 2001, pp. 109–128.

Secretary's Advisory Committee on Human Research Protections, "Considerations and Recommendations Concerning Internet Research and Human Subjects Research Regulations, with Revisions," Rockville, Md.: Office for Human Research Protections, U.S. Department of Health and Human Services, March 13, 2013. As of March 16, 2017: https://www.hhs.gov/ohrp/sites/default/files/ohrp/sachrp/mtgings/2013%20March%20Mtg/internet_research.pdf

Spencer, Robert, "Stage-Managed Massacre," *FrontPageMag*, August 2, 2006. As of March 16, 2017: http://archive.frontpagemag.com/readArticle.aspx?ARTID=3281

Taipale, K. A., "The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance," *Yale Journal of Law and Technology*, Vol. 9, Spring 2007, pp. 128–161.

U.S. Department of Defense Directive 5400.11, *DoD Privacy Program*, October 29, 2014.

U.S. Department of Defense Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, August 8, 2016.

U.S. House of Representatives, Committee on Armed Services, report on H.R. 4909, National Defense Authorization Act for Fiscal Year 2017, with additional views, Washington, D.C., May 4, 2016. As of March 16, 2017: https://www.congress.gov/114/crpt/hrpt537/CRPT-114hrpt537.pdf

Vautrinot, Suzanne M., "Sharing the Cyber Journey," *Strategic Studies Quarterly*, Vol. 6, No. 3, Fall 2012, pp. 71–87.

Wall, Andru E., "Demystifying the Title 10–Title 50 Debate: Distinguishing Military Operations, Intelligence Activities and Covert Action," *Harvard National Security Journal*, Vol. 3, 2011, pp. 85–141.

Watts, Duncan J., and Peter Sheridan Dodds, "Influentials, Networks, and Public Opinion Formation," *Journal of Consumer Research*, Vol. 34, No. 4, December 2007, pp. 441–458.

Xiong, Fei, and Yun Liu, "Opinion Formation on Social Media: An Empirical Approach," *Chaos*, Vol. 24, No. 1, March 2014.

Zeitzoff, Thomas, "Does Social Media Influence Conflict? Evidence from the 2012 Gaza Conflict," *Journal of Conflict Resolution*, June 7, 2016.

Zeitzoff, Thomas, John Kelly, and Gilad Lotan, "Using Social Media to Measure Foreign Policy Dynamics: An Empirical Analysis of the Iranian-Israeli Confrontation (2012–13)," *Journal of Peace Research*, Vol. 52, No. 3, May 2015, pp. 368–383.

Zimmer, Michael, and Nicholas John Proferes, "A Topology of Twitter Research: Disciplines, Methods, and Ethics," *Aslib Journal of Information Management*, Vol. 66, No. 3, 2014, pp. 250–261.

تؤدي وسائل التواصل الاجتماعي دوراً مهمّاً ومتزايداً في الإعلانات والبحث الأكاديمي، ولكنّها تقترن أيضاً بقدرةٍ كامنةٍ كبيرةٍ على دعم عمليات المعلومات العسكرية الأمريكية من خلال توفير فهمٍ لمناظير مجموعة كبيرة من الجماهير ذات الصلة وأفكارها وأنماط تواصلها. وعلى الرغم من وجود أسبابٍ اضطراريّة مرتبطة بالأمن القومي لنشر القدرة على تحليل وسائل التواصل الاجتماعي، يتوجّب على وزارة الدفاع الأمريكية (U.S. Department of Defense [DoD]) القيام بذلك، مع مراعاة معايير قانونية وثقافية أمريكية وفي ظلّ ظروفٍ من عدم اليقين الكبير على حدّ سواء. لم تتوقّع أُطُر العمل الحالية القانونية والخاصة بالسياسات الوتيرة السريعة والوصول العالمي لشبكات التواصل الحديثة، وتعيق مسائل الكلفة والتنفيذ تطوير قدرةٍ صلبةٍ على تحليل وسائل التواصل الاجتماعي والتطبيقات الأكثر فائدةً لهذه التحليلات. وبهدف دعم تقييم وزارة الدفاع الأمريكية للمنافع، والمفاضلات، وتحديات التنفيذ التي ستواجهها وهي توسّع قدرتها على تحليل وسائل التواصل الاجتماعي، تراجع هذه الدراسة المقاربات التحليلية التي ستقترن بالقيمة الأكبر بالنسبة لعمليات المعلومات، بالإضافة إلى الاعتبارات القانونية والأخلاقية والمرتبطة بالسياسات والتكنولوجية والمرتبطة بالتدريب. وهو يشمل أيضاً مجموعة من التوصيات لمساعدة وزارة الدفاع الأمريكية في التنقّل في هذا المجال، مع بناء قدرةٍ تحليليةٍ صلبةٍ وفعالةٍ خاصّة بوسائل التواصل الاجتماعي من أجل دعم العمليات من حول العالم.

NATIONAL DEFENSE RESEARCH INSTITUTE RAND

www.rand.org

Arabic Translation
"Monitoring Social Media"
RR-1742/1-OSD