Global Network
on Extremism & Technology

لحظات الهجرة: تبني المتطرفين تطبيقات المراسلة الفورية النصية

بينيت كليفورد

مشروع GNET من المشرعات الخاصة التي يقدمها المركز الدولي لدراسة الراديكالية، كينجز كوليدج لندن.

كتب هذا التقرير بينيت كليفورد، كبير الزملاء الباحثين،
برنامج التطرف بجامعة جورج واشنطن

الشبكة العالمية للتطرف والتكنولوجيا (GNET) مبادرة بحثية أكاديمية يدعمها منتدى الإنترنت العالمي لمكافحة الإرهاب (GIFCT)، وهي مستقلة ولكن تمولها الصناعة من أجل فهم أفضل لاستخدام الإرهابيين للتكنولوجيا والتصدي لهم. ويقوم المركز الدولي لدراسة الراديكالية (ICSR) بتنظيم فعاليات الشبكة العالمية للتطرف والتكنولوجيا (GNET) والإشراف عليها، بصفته مركزًا بحثيًا أكاديميًا داخل قسم دراسات الحروب في كينجز كوليدج لندن. والآراء والاستنتاجات الواردة في هذه الوثيقة آراءُ المؤلفين، ولا تُفسر على أنها تمثل آراء منتدى الإنترنت العالمي لمكافحة الإرهاب (GIFCT) ولا الشبكة العالمية للتطرف والتكنولوجيا (GNET) ولا المركز الدولي لدراسة الراديكالية (ICSR)، سواء كانت صريحة أو ضمنية.

بيانات الاتصال

لأي أسئلة أو استفسارات، أو للحصول على نسخ أخرى من هذا التقرير، يرجى التواصل مع:

ICSR
King's College London
Strand
London WC2R 2LS
المملكة المتحدة

هاتف: **+44 20 7848 2098**
بريد إلكتروني: **mail@gnet-research.org**

تويتر: **@GNET_research**

هذا التقرير، كغيره من منشورات الشبكة العالمية للتطرف والتكنولوجيا (GNET)، يمكن تنزيله مجانًا من موقع شبكة GNET على الإنترنت www.gnet-research.org.

الملخص التنفيذي

- يستخدم المتطرفون ذوو القناعات المتعددة – ومنهم الجهاديون أنصار القاعدة وتنظيم الدولة الإسلامية في العراق والشام وكذلك العديد من الجماعات اليمينية المتطرفة – حاليًا تطبيق تليغرام للمراسلة الفورية النصية كمنتدى تنسيقي مركزي لأنشطتهم عبر الإنترنت. ومع ذلك، نظرًا لسياسات تليغرام الجديدة، والتعاون مع جهات إنفاذ القانون وشركاء الصناعة الآخرين، والإصرار على فرض شروط خدماتها، بات المتطرفون في مواجهة ضغوط كبيرة على نظامهم الإيكولوجي القائم على تطبيق تليغرام.

- ويواصل الجهاديون والمتطرفون اليمينيون المتشددون عبر الإنترنت تجريب تطبيقات المراسلة الفورية النصية الأخرى جنبًا إلى جنب مع تليغرام كبدائل محتملة. ومع ذلك، من المستبعد أن يتم الانتقال الشامل إلى أي منصة أخرى على المدى القصير. وبمقارنة تليغرام مع منافسيها، فإن مجموعة ميزات تليغرام وإقبال المتطرفين عليها وسهولة استخدامها تضمن استمرار التطرف في استغلال المنصة على الرغم من وجود أنظمة تنفيذية جديدة للشركة.

- وبالتزامن مع أنصار الجماعات المتطرفة في نضالها للبقاء على تليغرام، تحاول المجموعات أو تخطط لتعزيز وجودها على تطبيقات المراسلة الفورية النصية الأخرى. وفي هذا الصدد، حظيت ست منصات (BCM و Gab Chat و Hoop Messenger و Riot.im و Rocket.Chat و TamTam) باهتمام كبيرٍ من الجماعات المتطرفة خلال العامين الماضيين كبدائل محتملة لتطبيق تليغرام.

- ويوضح التحليل التالي أن المتطرفين أقبلوا على هذه المنصات بسبب مجموعات ميزاتها وسهولة استخدامها ومواقف الشركة المضيفة من الخصوصية والأمن وتنظيم المحتوى المتطرف.

- وهناك اتجاهان من المحتمل أن يحددا مستقبل الاستغلال المتطرف لتطبيقات المراسلة الفورية النصية:

  - من المرجح أن يبحث أنصار الجماعات المتطرفة التي عززت تواجدها إلى حد كبير على تليغرام عن منصات بها مجموعات من الميزات والإمكانيات والتخطيطات المرئية التي تتشابه للغاية مع تليغرام.

  - ومن المرجح أن يواصل أنصار الجماعات المتطرفة جهودهم لاستغلال منصات الرسائل الفورية النصية التي توفر خوادم لامركزية وإمكانية تخزين البيانات.

- لمواجهة الاستغلال المتطرف لتطبيقات الرسائل الفورية النصية، قد تنظر مبادرات الصناعة المشتركة، مثل منتدى الإنترنت العالمي لمكافحة الإرهاب، في تجميع موفري خدمة الرسائل الفورية النصية في منتديات قائمة بذاتها لتعزيز التعاون وتبادل المعلومات. وعمومًا، يجب على الباحثين وصانعي السياسات والقائمين بمكافحة التطرف عبر الإنترنت أن يفكروا في تبني نهج تركز على الميزات، بدلاً من النهج التي تركز على المنصات، لتقييم الاستغلال المتطرف لتقنيات الاتصالات الرقمية.

المحتويات

1 مقدمة: المتطرفون، وتليغرام، والانتقال

يبحث هذا التقرير خليطًا من تطبيقات المراسلة الفورية النصية عبر الإنترنت التي تفضلها الجماعات الجهادية واليمينية المتطرفة المتشددة، مع التركيز على تخطيط ميزانياتها الفنية ومواقف الشركات المضيفة لها بشأن خصوصية المستخدمين وأمنهم وتنظيمهم. ولهذا يحلل التقرير ست خدمات للمراسلة عبر الإنترنت (BCM و Gab Chat و Hoop Messenger و Riot.im و Rocket.Chat و TamTam) التي تستخدمها أو قد تستخدمها الجماعات المتطرفة مع تليغرام.

وفيما يركز كثيرون من أنصار الجماعات المتطرفة المختلفة حاليًا على خدمة تليغرام للمراسلة الفورية عبر الإنترنت، يسعى آخرون إلى منصات أخرى.[1] وكثيرًا ما يُشار إلى تليغرام بأنها "المنصة المفضلة" للجهاديين عبر الإنترنت، وخصوصًا أنصار تنظيم الدولة الإسلامية في العراق والشام (تنظيم داعش)، كما أنها تحظى باستمرار بشعبية بين حركات اليمين البالغة التطرف.[2] ويعتبر المحللون وخبراء التطرف عبر الإنترنت، وحكومات عديدة، أن تليغرام منصة ثابتة لاتصالات الجماعات المتطرفة ذات القناعات المتعددة بسبب ما تقدمه من ميزات، بما فيها تشفير اتصالات مستخدميها من النهاية إلى النهاية وضمانات عدم الكشف عن هويتهم وحماية خصوصيتهم.[3] ويستخدم المتطرفون قنوات ومجموعات تليغرام كنقطة انطلاق إلى "عصر المنصات المتعددة"، حيث يُعاد بث محتوى الوسائط من تليغرام إلى منصات المراسلة الأخرى والمواقع الإلكترونية التي تخاطب الجماهير.[4]

ولكن التغييرات الأخيرة في شروط الخدمة وسياسات الخصوصية في تليغرام تُضعف الإمكانيات التي توفرها المنصة للجماعات المتطرفة. وعلى سبيل المثال، في أبريل 2018، أضافت تليغرام القسم 3.8 إلى سياسة خصوصيتها. وينص هذا القسم، الذي يعد خروجًا عن حظر تليغرام سابقًا تبادل المعلومات مع الحكومات، على الآتي "إذا تلقت تليغرام أمرًا من المحكمة يؤكد أنك مشتبه بالإرهاب، يجوز لنا كشف عنوان IP الخاص بك ورقم هاتفك للسلطات المختصة."[5] وبالتزامن مع هذا التغيير في سياسة خصوصيتها، بدأت تليغرام أيضًا مشاركتها في "أيام إجراءات الإحالة" التي نظمها اليوروبول وجهات إنفاذ القانون في الاتحاد الأوروبي.[6] وخلال يوم إجراء الإحالة الحادي عشر، اقتصر نطاق مشاركة تليغرام على مجرد مراقبة قيام جهات إنفاذ القانون الأوروبية باكتشاف المحتوى الإرهابي وتحديده.[7] ولكن خلال يوم إجراء الإحالة السادس عشر في نوفمبر 2019، تعاونت تليغرام مع يوروبول وشركاء الصناعة غوغل وتويتر وانستغرام.[8] وقامت المنصات معًا بإزالة 26,000 عنصرًا من دعاية داعش، بما فيها الحسابات والقنوات والمجموعات ومقاطع الفيديو والمنشورات الأخرى من مواقعها.[9]

---

1 Clifford, Bennett, and Helen Powell. 2019. "Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram." Washington, D.C.: Program on Extremism. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/EncryptedExtremism.pdf؛
Bloom, Mia, Hicham Tiflati, and John Horgan. 2019. "Navigating ISIS's Preferred Platform: Telegram." Terrorism and Political Violence 31 (6): 1242–1254. https://doi.org/10.1080/09546553.2017.1339695؛
Bloom, Mia, and Chelsea Daymon. 2018. "Assessing the Future Threat: ISIS's Virtual Caliphate" Orbis 62 (مايو). https://doi.org/10.1016/j.orbis.2018.05.007؛
"Telegram: The Latest Safe Haven for White Supremacists." 2019. Anti-Defamation League. 2 ديسمبر 2019. https://www.adl.org/blog/telegram-the-latest-safe-haven-for-white-supremacists.

2 Anti-Defamation League, "Telegram: The Latest Safe Haven for White Supremacists".

3 Clifford and Powell, "Encrypted Extremism".

4 المرجع نفسه.

5 المرجع نفسه.

6 Amarasingam, Amarnath. 2020. "A View from the CT Foxhole: An Interview with an Official at Europol's EU Internet Referral Unit." CTC Sentinel 13 (2). https://ctc.usma.edu/view-ct-foxhole-interview-official-europols-eu-internet-referral-unit/.

7 "Referral Action Day with Six EU Member States and Telegram." 2018. Europol. 5 أكتوبر 2018. https://www.europol.europa.eu/newsroom/news/referral-action-day-six-eu-member-states-and-telegram.

8 "Europol and Telegram Take on Terrorist Propaganda Online." 2019. Europol. 25 نوفمبر 2019. https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online.

9 المرجع نفسه.

وتعليقًا على هذا الإجراء، زعم المتحدث باسم المدعي الفيدرالي البلجيكي إريك فان دير سيبت أن عملية الإزالة الجماعية جعلت تنظيم داعش "لم يعد موجودًا على الإنترنت" في الوقت الحالي.[10]

وبالرغم من التقييم الأولي الذي أجراه فان دير سيبت، احتفظت الجماعات المتطرفة بوجودها على تليغرام بعد أيام إجراء الإحالة. وفيما وجهت هذه العملية ضربة مؤقتة لأنصار تنظيم داعش على تليغرام، توصلت تحليلات الشبكة العالمية للتطرف والتكنولوجيا إلى بقاء "مخلفات عنيدة من وجودها الأساسي" في الخدمة، و "يستمر نشر الدعاية الرسمية وغير الرسمية لها بوتيرة ثابتة."[11] قام أنصار داعش، وهي الجماعة الوحيدة التي تستهدفها هذه الجهود فيما نعلم، بتعزيز وجودها بسرعة على العديد من منصات المراسلة الفورية البديلة عبر الإنترنت. وتمكن أنصار تنظيم داعش، من خلال اللامركزية، من البقاء على الإنترنت لأن "التشتت على هذه المنصات التي يزيد عددها عن اثنتي عشرة منصة يؤدي إلى انتشار الدعاية الجهادية اللامركزية أكثر وأكثر"، لكن تنظيم داعش "زاد من ظهوره" بنشر هذا المحتوى عبر الانترنت.[12] في يوليو 2020، أعلن تقييم أجراه يوروبول أن "الجهود المبذولة لتعزيز وجود داعش عبر الإنترنت مستمرة عبر العديد من المنصات، بما فيها تليغرام".[13] علق المسؤولون المشاركون في فعالية أيام الإحالة على تليغرام بأن هذه الجهود ركزت في الغالب على أنصار داعش، وتركت الجماعات الجهادية الأخرى وغيرها من المتطرفين العنيفين فلم تتأثر إلى حد كبير بالحملة.[14]

وخلال عمليات إزالة المحتوى المرتبط بداعش على تليغرام، حافظت الجماعات اليمينية المتطرفة المتشددة على وجودها الكبير على هذه المنصة فلم تعوقها جهود إزالة المحتوى إلى حد كبير.[15] ومع ذلك، قد تطرأ تغيرات بطيئة على هذه التلية. وقامت تليغرام في صيف هذا العام بتنسيق عمليات إزالة المحتوى الخاص بأبرز الجماعات والقنوات اليمينية المتطرفة والمتشددة على منصتها.[16] وأوقفت المنصة عددًا من أكثر القنوات اليمينية المتطرفة المتشددة عنفًا وكراهية، بما فيها Terrorwave Refined، وهي "محور مركزي" لليمين المتطرف العنيف على تليغرام، بالإضافة إلى القنوات المتصلة بجماعة Misanthropic Division و RapeKrieg.[17] على الرغم من عمليات الإزالة، لم تتأثر معظم القنوات اليمينية المتطرفة على تليغرام ويواصل مديرو القنوات المحذوفة جهودهم لنشر المحتوى على المنصة.[18] يبقى أن نرى إذا كان المتطرفون اليمينيون المتطرفون على تليغرام سيفكرون بجدية في استخدام منصة أخرى أو إذا قُدِّر لجهود تليغرام أن تستمر.

10 Zialcita, Paolo. 2019. "Islamic State 'Not Present On The Internet Anymore' Following European Operation." NPR.Org. 25 نوفمبر 2019. https://www.npr.org/2019/11/25/782712176/islamic-state-not-present-on-the-internet-anymore-following-european-operation.

11 Gluck, Raphael. 2020. "Islamic State Adjusts Strategy to Remain on Telegram." Insight الشبكة العالمية للتطرف والتكنولوجيا. https://gnet-research.org/2020/02/06/islamic-state-adjusts-strategy-to-remain-on-telegram/; Creizis, Meili. 2020. "Telegram's anti-IS Campaign: Effectiveness, Perspectives, and Policy Suggestions." Insight الشبكة العالمية للتطرف والتكنولوجيا. https://gnet-research.org/2020/07/30/telegrams-anti-is-campaign-effectiveness-perspectives-and-policy-suggestions/

12 "Jihadists Presence Online Decentralizes After Telegram Ban." 2020. Flashpoint. 17 يناير 2020. https://www.flashpoint-intel.com/blog/terrorism/jihadists-presence-online-decentralizes-after-telegram-ban/.

13 "Online Jihadist Propaganda: 2019 in Review." 2020. Europol. 28 يوليو 2020. https://www.europol.europa.eu/sites/default/files/documents/report_online_jihadist_propaganda_2019_in_review.pdf.

14 Amarasingam, "A View from the CT Foxhole."

15 Katz, Rita. 2020. "Neo-Nazis Are Running Out of Places to Hide Online." WIRED، 9 يوليو 2020. https://www.wired.com/story/neo-nazis-are-running-out-of-places-to-hide-online/.

16 المرجع نفسه.

17 المرجع نفسه.

18 المرجع نفسه.

2 تطبيقات المراسلة الفورية النصية: فئات التحليل

من المستبعد على المدى القصير انسحاب المتطرفين عبر الإنترنت وهجرتهم الجماعية على نطاق واسع من تليغرام إلى منصة أخرى. ومع ذلك، هناك حاجة لفهم منصات المراسلة البديلة التي تستخدمها الجماعات المتطرفة بالإضافة إلى تليغرام. ولا يتخذ المتطرفون قرارات "إما/أو" بشأن استخدام المنصات؛ وكثيرًا ما يستغلون منصات متعددة في نفس الوقت.[19] على غرار تجارب المتطرفين في تليغرام حينما كانت تويتر وفيسبوك ترحبان بهم، من المرجح أن يقوم المتطرفون بتجربة منصات المراسلة الثانوية وإن ظلت تليغرام ترحب بهم. وعلاوة على ذلك، فإن تحليل هذه المنصات الثانوية ومقارنتها مع تليغرام يساعدنا في إبراز أكثر ميزات منصات المراسلة جذبًا للجماعات المتطرفة. وإذا افترضنا أن تليغرام تواصل بذل جهودٍ كبيرة وجريئة لإخلاء منصاتها من المتطرفين، فمن الضروري أن يفهم الممارسون آليات عمل المنصات الثانوية لاحتواء ما يترتب على حملات الإزالة من تأثيرات الدرجة الثانية، مثل هجرة المتطرفين إلى المنصات التي تتسم بضعف أجوائها التنظيمية، أو تزايد ترحيبها بالمتطرفين أو سياسات الخصوصية والأمان التي تحمي رسائل المتطرفين من تطبيق القانون أو سلطة الاستخبارات أو المنصات ذاتها.

من الواضح أن منصات الرسائل الفورية النصية التي تستخدمها الجماعات المتطرفة اليوم لا تقتصر على المنصات الست التي استعرضناها في هذا التحليل. ومع ذلك، تصارع كلٌ منها لمنع المتطرفين من استغلال خدماتها في السنوات الأخيرة؛ وتساعدنا المقارنة بين مختلف المنصات في كشف بعض المزايا الحيوية التي تعتبر مهمة عند اختيار هذه الجماعات منصات المراسلة الفورية النصية. وتبحث هذه الورقة العوامل الخمسة التي تمكِّن كل منصة من تحديد نهجها العام في التعامل مع المحتوى المتطرف: الاستخدام المتطرف، ومجموعات الميزات، وسهولة وصول المستخدم، والخصوصية والأمن، ومشهد السياسات/القواعد التنظيمية. وتستدعي كل فئة من هذه الفئات الخمس ثمة أسئلة رئيسية عن استخدام الجماعات المتطرفة منصات المراسلة الفورية:

- الاستخدام المتطرف: ما أنواع الجماعات المتطرفة التي تستخدم المنصة؟ متى بدأت استخدام المنصة؟ هل تستخدم المنصة حاليًا؟ ما مدى التطرف في استخدام المنصة؟

- مجموعة الميزات: ما الميزات التي توفرها هذه المنصة؟ أيٌ من هذه الميزات يميزها عن منافسيها، لاسيما عندما يتعلق الأمر بالاستخدام المتطرف للمنصة (أو بإساءة استخدامها)؟

- سهولة وصول المستخدم: ما مدى سهولة استخدام المنصة؟ ما الخطوات اللازمة لإنشاء حساب عليها والوصول إلى محتوى معين؟ ما هي البروتوكولات التي يعمل النظام وفقًا لها؟ هل المنصة عرضة للخلل أو محاولات القرصنة أو غيرها من جهود رفض تقديم الخدمة؟

- الخصوصية والأمن: ما هو وضع خصوصية المستخدم في شروط خدمة المنصة؟ هل توفر التشفير؟ أين تخزِّن بيانات المستخدم؟ من هم الأطراف الآخرون الذين يمكنهم الوصول إلى بيانات المستخدم؟

19 Prucha, "IS and the Jihadist Information Highway"; Alkhouri, Laith, and Alex Kassirer. 2016. "Tech for Jihad: Dissecting Jihadists Digital Toolbox." Flashpoint. https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf; Conway, Maura. 2006. "Terrorism and the Internet: New Media – New Threat?" Parliamentary Affairs 59 (2): 283–98. https://doi.org/10.1093/pa/gsl009.

- مشهد السياسات/القواعد التنظيمية: ما هي سياسة المنصة بشأن إزالة المحتوى الإرهابي والمتطرف؟ هل تُصدر تقارير عن الشفافية؟ أين سُجلت المنصة وما هي قوانين تنظيم المحتوى التي تخضع لها؟ ما علاقتها بطلب الجهات الحكومية الاطلاع على بيانات المستخدم؟

وفي القسم الأخير، يسلط التقرير الضوء على أكثر الميزات شيوعًا في هذه المنصات لإيضاح أشد الميزات جذبًا للجماعات المتطرفة. ويدعو إلى تحليل استخدام المتطرفين للإنترنت ومكافحته باتباع نهج يركز على الميزات، وليس على المنصة.

3 استخدام المتطرفين تطبيقات المراسلة الفورية النصية الثانوية

يُحلل هذا القسم ستًا من منصات المراسلة الفورية النصية التي يستغلها أو قد يستغلها المتطرفون بعد تشديد تليغرام الالتزام بشروط الخدمة. وبعد ستة أشهر من أيام إجراء إحالة تليغرام، خلُص تقرير أجراه يوروبول إلى أن الجهاديين المنتمين إلى داعش على الإنترنت، بعد أن تعرضوا لموجة من الإزالات، "توافدوا إلى منصة TamTam و Hoop Messenger" بينما كانوا يختبرون "تطبيقات هامشية، مثل Blockchain messenger BCM و RocketChat وبرنامج المراسلة الفورية Riot المجاني."[20] وعكف نظراؤهم في الجماعات الجهادية الأخرى، وكذلك في الجماعات اليمينية المتطرفة، على تجربة العديد من هذه المنصات. وفضلاً عن هذه المنصات الخمس، يحلل القسم منصة إضافية أخرى، Gab Chat، وهي قيد التطوير حاليًا ولكن لديها من الإمكانيات وإرث الشركة المضيفة ما قد يجذب المتطرفين اليمينيين.[21]

BCM Messenger

الـ BCM Messenger ("لأن التواصل مهم") تطبيق لامركزي للمراسلة كان يقدم خدمة الدردشات الخاصة والدردشات الجماعية لنحو 100,000 مشترك.[22] وهناك غموض حول مَنشأ هذه الشركة، فقد أنشأ المنصة مطورون صينيون وسُجلت في جزر فيرجن البريطانية كبديل لامركزي لمنصة المراسلة الصينية WeChat.[23] ولاحظ العديد من مراقبي وسائل الإعلام المتطرفة عبر الإنترنت إقبال أنصار داعش على تجريب هذا التطبيق في أعقاب أيام إجراء إحالة عام 2019.[24] على سبيل المثال، أنشأت وكالة ناشر الإخبارية، إحدى الشبكات الإعلامية عبر الإنترنت التابعة لتنظيم داعش، عدة قنوات على المنصة في ديسمبر 2019.[25] في فبراير 2020، أخطرت الشركة المستخدمين بأنها أوقفت خدمة المراسلة.[26]

ميزت BCM نفسها عن تليغرام وغيره من برامج المراسلة الفورية عبر الإنترنت بطرق عديدة. أولها، وأهمها، أنها تعمل على نموذج خادم لامركزي. وبخلاف خدمات المراسلة الأخرى التي تخزن بيانات المستخدم ومعلوماته على خوادم مركزية يتحكم فيها مزود الخدمة، قامت BCM وغيرها من الأنظمة اللامركزية بتوزيع نقاط الخادم عبر شبكة المستخدمين، ما أتاح لكل مستخدم إمكانية تخزين بياناته والتحكم في الوصول إليها.[27] بينما توفر بعض برامج المراسلة الفورية عبر الإنترنت تقنية التشفير من النهاية إلى النهاية لبعض أشكال الاتصالات (وليس كلها) أو تستطيع توفيرها بالطلب

20 "Europol, "Online Jihadist Propaganda: 2019 in Review.

21 Morse, Jack. 2020. يتضح من الوثائق المسربة "قلق الشرطة من تنظيم المتطرفين البيض على Gab Chat". 13 يوليو 2020. https://mashable.com/article/law-enforcement-documents-violent-white-extremists-encrypted-gab-chat/.

22 "BCM Messenger." بلد تاريخ. BCM Messenger. تم الوصول في 1 أبريل 2020. "Privacy Policy"، بلد تاريخ. BCM Messenger. تم الوصول في 1 أبريل 2020. وخدمة BCM موقوفة الآن. ويمكنكم الاطلاع على إصدارات الصفحة وسياسة خصوصية BCM باستخدام Wayback Machine على https://bcm.social/index.html/https://web.archive.org/web/20200215082731 و https://bcm.social/license/policy.html/https://web.archive.org/web/20191016053505.

23 المرجع نفسه؛ Yuan, Lanny, Huaibing Jian, Peng Liu, Pengxin Zhu and ShanYang Fu. 2018. "AME Blockchain: An Architecture Design for Closed-Loop Fluid Economy Token System." White Paper.

24 Smith, Brenna. 2019. "Terrorists Use a New Blockchain Messaging App after Telegram Crackdown." Bellingcat CryptOSINT. 10 ديسمبر 2019. https://mailchi.mp/7884c14d5fb9/terrorists-use-a-new-blockchain-messaging-app-after-telegram-crackdown.

25 المرجع نفسه؛ Flashpoint, "Jihadists Presence Online Decentralizes After Telegram Ban"؛ Gluck, "Islamic State Adjusts Strategy to Remain on Telegram"؛ Webb, Sam, and Colin Rivet. 2019. "Terror Group ISIS Testing Blockchain Messaging App". 16 ديسمبر 2019. https://finance.yahoo.com/news/terror-group-isis-testing-blockchain-150028142.html.

26 رسالة إلى مشتركي BCM، 22 فبراير 2020. https://postimg.cc/3dWTwGmp.

27 Yuan et. al. "AME Blockchain: An Architecture Design for Closed-Loop Fluid Economy Token System."

فقط، تُشفَّر الرسائل المرسلة عبر BCM افتراضيًا.[28] بخلاف ذلك، تتشابه BCM مع تليغرام في مجموعة ميزاتها (المحادثات الخاصة والجماعية) وخوارزمية التشفير التي تستخدمها.[29]

ويستطيع المستخدم إنشاء حساب في BCM بمجرد تنزيل التطبيق وتسجيل المعرف الخاص به. وبخلاف تليغرام، لا يتطلب التسجيل وجود رقم الهاتف.[30] ويتطلب الوصول إلى مجموعات معينة وجود رابط الموقع الإلكتروني إلى المحتوى، ويتطلب الاتصال بالمستخدمين الآخرين مباشرةً معرفة مفتاحهم العام أو معرفاتهم كمستخدمين للـ BCM. وكان تطبيق BCM مبنيًا على "بنية أساسية غير مركزية ومنصة تطبيقات" تسمى AME صُممت على أساس مبدأ "عدم الثقة": "تطبيق BCM لا يثق بأحد إلا نفسه، ولا حتى بخادم BCM".[31] لم يتمكن أي طرف ثالث، بما في ذلك خادم BCM نفسه، من فك تشفير الرسائل المرسلة بين المستخدمين. كما تقدم BCM محفظة للعملات المشفرة بالإضافة إلى خدمة المراسلة الفورية التي لا تزال توفرها بالرغم من إغلاقها.[32] ولذلك أخطأ من ادعى أن خدمة المراسلة الفورية كانت "مبنية على سلسلة كتل (blockchain)"، لأن المحفظة الرقمية فقط هي التي كانت مبنية على سلسلة كتل.[33]

ووفقًا لسياسة خصوصية BCM، "لن تستخدم الشركة [بيانات المستخدم] ولن تفصح عنها للغير إلا بإذن مسبق منك."[34] من المستحيل أن تتمكن الشركة من فك تشفير الرسائل المتبادلة بين المستخدمين بفضل منصتها اللامركزية وتوفير خدمة التشفير الافتراضي من النهاية إلى النهاية لجميع الاتصالات. ولأن بيانات المستخدمين تُخزن بواسطة عُقد فردية في الشبكة، فمن الصعب تلبية طلب الوصول إلى الخوادم من باب تطبيق القانون.[35] لم تصدر الشركة أي توجيهات بشأن خطة تصديها للمحتوى الإرهابي أو المتطرف، ولكن علق أحد المتحدثين باسم الشركة قائلاً فيما تلتزم الشركة بقوانين السلطات القضائية المحلية، "لن نلبي بأي حال من الأحوال أي مطالب بفك التشفير وأسرار وخفايا مراقبة المحتوى."[36]

خدمة الدردشة Gab Chat

تأسست شبكة Gab في عام 2016 "كبديل في حرية التعبير" لتويتر؛ وزعم الشريك المؤسس، أندرو توربا، أن الدافع الرئيسي لإنشاء هذه المنصة هو "الاحتكار الاجتماعي الكبير ذو الميول اليسارية".[37] وذاعت سمعتها السيئة كونها نقطة لحشد المتطرفين اليمينيين المتشددين عبر الإنترنت وأثارت أسئلة عديدة عندما اتضح أن مرتكب حادث إطلاق النار في أكتوبر 2018 في كنيس تري أوف لايف في بيتسبرغ كان قد انضم إلى مجتمع هامشي من النازيين الجدد على المنصة.[38] وما كان من مزودي خدمات Gab المتعددين إلا أن أوقفوا تقديم خدماتهم إلى هذا الموقع.[39] وبعد أن تنقلت Gab بين شركات الاستضافة، احتفظت بأكثر من 1,000,000 حساب ومجتمع ثابت يضم متطرفين يمينيين.[40]

في أواخر يناير 2020، أعلنت Gab أنها في المراحل الأولى من طرح منصة للمراسلة الفورية على غرار تليغرام، تسمى Gab Chat.[41] وأعلنت أن هذه الخدمة عبارة عن

---

28 "FAQ". بلا تاريخ. BCM Messenger. تم الوصول في 1 أبريل 2020. https://web.archive.org/web/20200115224708/https://bcm.social/faq.html.
29 المرجع نفسه.
30 المرجع نفسه.
31 المرجع نفسه.
32 المرجع نفسه.
33 المرجع نفسه.
34 BCM Messenger, "Privacy Policy."
35 المرجع نفسه.
36 المرجع نفسه.
37 Lorenz, Taylor. 2018. "The Pittsburgh Suspect Lived in the Web's Darkest Corners." The Atlantic. 27 أكتوبر 2018. https://www.theatlantic.com/technology/archive/2018/10/what-gab/574186/.
38 المرجع نفسه.
39 Jurecic, Quinta. 2018. "Gab Vanishes, and the Internet Shrugs." Lawfare. 29 أكتوبر 2018. https://www.lawfareblog.com/gab-vanishes-and-internet-shrugs.
40 "When Twitter Bans Extremists, GAB Puts Out the Welcome Mat." 2019. Anti-Defamation League. 11 مارس 2019. https://www.adl.org/blog/when-twitter-bans-extremists-gab-puts-out-the-welcome-mat.
41 Torba, Andrew. 2020. "AG Barr Is Wrong On Encryption. Introducing Gab Chat: An Open Source Encrypted Messaging Platform." Gab News (blog). 31 يناير 2020. https://news.gab.com/2020/01/31/ag-barr-is-wrong-on-encryption-introducing-gab-chat-our-open-source-encrypted-messaging-platform/.

"خدمة مراسلات ودردشة مشفرة ومزودة بغرف دردشة عامة وخاصة."[42] وزعم توربا أن غرف الدردشة العامة، مثل تليغرام، لن تقدم تشفيرًا افتراضيًا لجميع الاتصالات، لكن الدردشات الخاصة ستكون مشفرة من النهاية إلى النهاية: "لا يستطيع قراءة الغرف المشفرة إلا الأعضاء في غرفة الدردشة، ولا حتى Gab."[43] علاوة على ذلك، لن يُستضاف تطبيق Gab Chat إلا على موقع Gab الإلكتروني وليس متاجر التطبيقات الشهيرة التي توفرها غوغل و آبل.[44]

والميزة الأساسية في منصة Gab للمتطرفين هي ضمان الشركة عدم إدارة المحتوى أو إزالته. وأنها تعتبر إتاحة حرية التعبير أمرًا مقدسًا وتفتخر بسياستها المناهضة لفرض الرقابة.[45] ومع ذلك، "في حالة اكتشاف تهديد غير قانوني على المنصة، أو إذا علمنا بحدوث سلوك خطير عنيف خارج المنصة من فرد ربما يكون قد أنشأ حسابًا على موقعنا"، فإن الشركة سوف "[تتعاون] و [تتواصل] مع جهات إنفاذ القانون الفيدرالية والمحلية والولاياتية باستمرار ... لمساعدتها في منع الجرائم الخطيرة."[46]

وما زالت Gab Chat في مرحلة التجريب.[47] وإذا وضعنا في اعتبارنا شعبية Gab بين المتطرفين اليمينيين كبديل لمقدمي وسائل التواصل الاجتماعي الجماهيرية مثل تويتر و فيسبوك، فمن المنطقي أن نتوقع تبني بعض المتطرفين Gab Chat. يُضاف إلى هذا شعبية خدمة تليغرام وما كان على شاكلتها من خدمات بين المتطرفين اليمينيين. وإذا كانت Gab Chat تقدم خدمات مماثلة لخدمات تليغرام تحت راية Gab، فقد يعتبرها المتطرفون اليمينيون المتشددون منصة مضيافة للمراسلة الفورية عبر الإنترنت ويحاولون استغلال المنصة عندما تعمل بكامل طاقتها.

خدمة المراسلة Hoop Messenger

خدمة Hoop Messenger عبارة عن تطبيق للمراسلة الفورية عبر الإنترنت، على غرار تليغرام، يوفر خيارات للتواصل في صورة دردشات خاصة وغرف دردشة وقنوات من واحد إلى متعدد. وتقوم بتشغيلها شركة صغيرة في كندا.[48] في ديسمبر 2019، بعد جهود إزالة وسائل الإعلام المرتبطة بداعش بتنسيق من اليوروبول، أنشأت العديد من المنافذ الإعلامية الرسمية وغير الرسمية التابعة لتنظيم داعش والقاعدة قنوات على Hoop Messenger، ومن أنصارهما مَن شجع استخدام المنصة كبديل آمن لتليغرام.[49] وبعد أيام، أزالت الشركة عددًا كبيرًا من القنوات المرتبطة بتنظيم داعش على منصتها.[50] وفي أواخر يناير 2020، حذرت مؤسسة إعلامية موالية لتنظيم داعش متابعيها من استخدام Hoop Messenger، مدعية أنه يجمع معلومات شخصية كثيرة من المستخدمين.[51]

واليوم، لا تزال داعش تحظى بحضور كبير على Hoop Messenger. ويرى بعض أنصار داعش البارزين أن هذا الخيار قد يكون أكثر الخيارات جاذبية كبديل لتليغرام حاليًا. وفي أوائل يونيو 2020، أصدرت قناة وكالة ناشر الإخبارية على تليغرام رسالة "عاجلة" لمتابعيها مفادها أن Hoop Messenger سيكون قناتها الأساسية لنشر الأخبار.[52] جاء هذا الإعلان بعد الضغوط المستمرة على القنوات الموالية لتنظيم داعش على تليغرام.

---

42 المرجع نفسه.
43 المرجع نفسه.
44 المرجع نفسه.
45 Torba, Andrew. 2019. "Gab's Policies, Positions, and Procedures for Unlawful Content And Activity On Our Social Network." Gab News (blog). 23 أغسطس 2019. https://news.gab.com/2019/08/23/gabs-policies-positions-and-procedures-for-unlawful-content-and-activity-on-our-social-network/.
46 المرجع نفسه.
47 Torba, "AG Barr is Wrong on Encryption."
48 "FAQ". بلد تاريخ، خدمة المراسلة Hoop Messenger. تم الوصول في 1 أبريل 2020. http://hoopmessenger.com/faq/.
49 Amarasingam, Amarnath. 2019. "Telegram Deplatforming ISIS Has Given Them Something to Fight For." Vice. 5 ديسمبر 2019. https://www.vice.com/en_us/article/vb55bd/telegram-deplatforming-isis-has-given-them-something-to-fight-for; Bloom, Mia. 2019. "No Place to Hide, No Place to Post: Lessons from Recent Efforts at 'De-Platforming' ISIS." Just Security. 5 ديسمبر 2019. https://www.justsecurity.org/67605/no-place-to-hide-no-place-to-post-lessons-from-recent-efforts-at-de-platforming-isis/; Seldin, Jeff. 2019. "IS Struggles to Regain Social Media Footing After Europe Crackdown." Voice of America. 4 ديسمبر 2019. https://www.voanews.com/europe/struggles-regain-social-media-footing-after-europe-crackdown.
50 المرجع نفسه.
51 "Pro-ISIS Media Foundation Warns ISIS Supporters Against Using Hoop Messenger." 2020. MEMRI. 27 يناير 2020. https://www.memri.org/cjlab/pro-isis-media-foundation-warns-isis-supporters-against-using-hoop-messenger.
52 "ISIS Media Outlet Announces Shift To Canadian Hoop Messenger App After Wave Of Account Deletions On Telegram." MEMRI. 5 يونيو 2020. https://www.memri.org/cjlab/isis-media-outlet-announces-shift-canadian-hoop-messenger-app-after-wave-account-deletions.

وفي الأيام التي أعقبت الإعلان، استورد أنصارها عددًا كبيرًا من القنوات المؤيدة لتنظيم داعش من تليغرام إلى Hoop Messenger.[53] وأصدرت مؤسسة Electronic Horizons التابعة لتنظيم داعش، والمسؤولة عن إنتاج المحتوى الخاص بالأمن الرقمي والتشغيلي، دليلاً لمشتركيها عن كيفية استخدام Hoop Messenger بأمان.[54] وبالرغم من هذه الجهود، استجاب Hoop Messenger بدوره بإطلاق حملة أخرى لإزالة المحتوى الموالي لتنظيم داعش عن منصته.[55]

ويتميز Hoop Messenger عن غيره من خدمات المراسلة الفورية بميزة "Vault"، وهو نظام لتخزين الملفات محمي بكلمة مرور ويتيح للمستخدمين إمكانية حفظ الدردشات والصور ومقاطع الفيديو والملفات الأخرى. وما أن ينشيء المستخدم كلمة مرور، تُشفَّر جميع الدردشات والملفات المحفوظة في نظام Vault من النهاية إلى النهاية على كلٍ من جهاز المستخدم والسحاب؛ أما القنوات وجميع الدردشات الأخرى فإنها غير مشفرة من النهاية إلى النهاية.[56] ويستطيع المستخدمون أيضًا إنشاء كلمات مرور زائفة لنظام Vault الخاص بهم، وبمجرد إدخالها، تتلف محتويات Vault ذاتيًا.[57] من خلال موقع الخدمة الإلكتروني، يتوفر للمستخدمين أيضًا خيار حذف حساباتهم عن بُعد، ما يؤدي إلى حذف نهائي لجميع البيانات الموجودة على حساب المستخدم والبيانات الشخصية المخزنة على هواتفهم.[58] ووفقًا للشركة، فإن كلمات المرور الوهمية لنظام Vault والإتلاف الذاتي للبيانات ميزتان مفيدتان لاسيما إذا "دخلت أماكن يُطلب منك فيها تسليم هاتفك ... ما عليك سوى حذف Hoop وتنزيله مرة أخرى بمجرد إعادته إليك بأمان."[59]

ويتطلب إنشاء حساب في Hoop Messenger التسجيل برقم هاتف و/أو عنوان بريد إلكتروني. وبخلاف بعض المنصات الأخرى، يستطيع المستخدمون إنشاء معرفات مستخدمين متعددة للحساب الواحد.[60] الاشتراك في الدردشات مطلوب للحصول على تشفير النهاية إلى النهاية الذي لا يمكن إجراؤه إلا من خلال نظام Vault، لكن Hoop Messenger يوفر أيضًا متصفح شبكة افتراضية خاصة (VPN) في خدمته ليتمكن المستخدمون من تصفح الويب من التطبيق دون مراقبة.[61] وتتشابه هذه المنصة مع تليغرام في هيئتها ووظائفها.

وتحدد الأقسام 9 و 10 و 11 من شروط خدمة Hoop Messenger طريقة تعاملها مع المحتوى الضار. وتحظر الخدمة "السلوك المرفوض والمحتوى غير المقبول"، وتشير إلى أن الشركة ستزيل أي محتوى أو حساب لمستخدم ينتهك شروط الخدمة.[62] في ديسمبر 2019، أوضحت الشركة أن هذه الإجراءات تنطبق على المحتوى الإرهابي، وزعمت أن الشركة "سوف تواصل إغلاق الجماعات المرتبطة بداعش" بعد حذف عدد كبير من القنوات والدردشات الموالية لتنظيم داعش من المنصة.[63] ونظرًا لما تقوم به الشركة من إجراءات منسقة ضد المحتوى والحسابات المتعلقة بتنظيم داعش، أعرض بعض أنصاره فيما يبدو عن استخدام Hoop Messenger، وحذروا غيرهم من استخدامه.[64] ومع ذلك، مِن أنصار داعش مَن لا يزال مقتنعًا بأن المنصة هي أفضل البدائل المتاحة لتليغرام.

---

53 المرجع نفسه.

54 Gluck, Raphael. 2020. "من عروض آفاق (AFAQ) الأخيرة – برنامج تعليمي عن كيفية استخدام Hoop Messenger بأمان – التطبيق الجديد الذي تحول إليه تنظيم داعش بعد تواصل عمليات الحذف من تليغرام. – مجلة "The Supporters Security"، تنشر الوعي الأمني بين محاربي لوحة المفاتيح – فيديو تعليمي من Debian." تغريدة، 3 يوليو 2020. https://twitter.com/einfal/status/1279124715957891072.

55 Alkhouri, Laith. 2020. "تمت إزالة العديد من قنوات #تنظيم داعش الرسمية وغير الرسمية من منصة Hoop Messenger التي تفضلها الجماعة في اتصالاتها/الدعاية لها. ولم يؤثر ذلك على توزيع وسائل تواصل الجماعة إلا بقدر ضئيل جدًا لأنها أنشأت عشرات القنوات الاحتياطية مبكرًا." تغريدة، 6 أغسطس 2020. https://twitter.com/MENAanalyst/status/1291415487453302790.

56 Hoop Messenger, "FAQ".

57 المرجع نفسه.

58 المرجع نفسه.

59 "Hoop Messenger". بلا تاريخ. خدمة المراسلة Hoop Messenger. تم الوصول في 1 أبريل 2020. http://hoopmessenger.com/.

60 المرجع نفسه.

61 المرجع نفسه.

62 "Privacy & Terms". بلا تاريخ. خدمة المراسلة Hoop Messenger. تم الوصول في 1 أبريل 2020. http://hoopmessenger.com/legal/.

63 @HoopMessenger, 2019. "We will continue shutting down ISIS-related groups. We encourage everyone to send us suspicious channels via email. Since our team is quite small we are relying on the public to help us. If there are any questions please reach out to our team via email or DM" 5 ديسمبر 2019. https://twitter.com/HoopMessenger/status/1202698188160811008.

64 MEMRI, "Pro-ISIS Media Foundation Warns ISIS Supporters Against Using Hoop Messenger."

تطبيق Riot.im

تطبيق Riot.im (أعيدت تسميته Element في يوليو 2020) هو تطبيق لامركزي للدردشة مبني على شبكة Matrix.[65] ويقدم خدمة الاتصالات في صورة دردشات ومجموعات واحد إلى واحد، وميزة تبادل الملفات ويمنح المستخدمين خيار التحكم في الوصول إلى الاتصالات.[66] وكان تصميمه في البداية كمنصة للتعاون المكتبي ويتشابه هيكليًا مع غيره من تطبيقات المراسلة الفورية في تلك الفئة (مثل Slack و Twist و Microsoft Teams).[67] وخلال فترة تجريبه مع منصات الويب اللامركزية، بدأ أنصار تنظيم داعش أولاً، ومن بعدهم بوقت قصير أنصار تنظيم القاعدة وغيرهم من أنصار الجهاديين، في إنشاء مجموعات على المنصة في سبتمبر 2017.[68] وحافظت هذه المجموعات على استمرار وجودها على المنصة منذ عام 2017.[69] ولكن، نظرًا لأن معظم أنصارهم فضلوا تخزين اتصالاتهم على خادم الشركة العام، فهناك خلل مستمر في الشبكات الجهادية على خوادم Riot.im بسبب إزالة المحتوى وجهود إزالة الحسابات.[70] ولاحظ مراقبو الجماعات اليمينية المتطرفة على الإنترنت أيضًا أن بعض القنوات اليمينية المتطرفة البارزة على تليغرام بدأت أيضًا في ترسيخ وجودها على Riot.im.[71]

ونظرًا لتأسيسها على منصة Matrix اللامركزية، شعر مراقبو النشاط المتطرف عبر الإنترنت بالقلق من أن Riot.im "قد يصبح الإصدار المحسن التالي من تليغرام" إذا فضل المتطرفون استضافة خوادمهم الخاصة بهم.[72] وكخيار، يقدم Riot.im للمستخدمين إمكانية تخزين اتصالاتهم على خادم matrix.org العام، أو على خادم متميز ومدفوع يستضيفه المستخدم بنفسه (أو مؤسسته)، أو على خوادم عامة أخرى يُنشئها مستخدمو Riot.im أو على خوادم مخصصة.[73] وبالتالي، بينما توفر المنصة خوادم لامركزية، فإنها تطلب من المستخدم نفسه المشاركة في الخادم ثم إدارته. وبغض النظر عن الاتصالات سواءً كانت مخزنة على خادم عام مركزي أو خادم لامركزي، يستطيع المستخدمون تفعيل تشفير اتصالاتهم على Riot.im من النهاية إلى النهاية.[74]

ويتطلب التسجيل للحصول على حساب Riot.im إنشاء اسم مستخدم وكلمة مرور، ويستطيع المستخدمون أيضًا أن يختاروا استخدام عنوان البريد الإلكتروني.[75] وبعد إنشاء الحساب، يستطيع صاحب الدردشة تغيير إعداداتها بحيث لا يتمكن من المشاركة فيها إلا مستخدمون محددون فقط، ولا يستطيع الوصول إلى الدردشة أو إتاحتها للعامة إلا المستخدمون الذين لديهم رابط للدردشة فقط.[76] يستطيع المشاركون أيضًا تفعيل تشفير الرسائل من النهاية إلى النهاية.

وتطبيق Riot.im مبني على منصة Matrix، وخوادمه العامة مستضافة على Matrix. وهاتان الخدمتان مقرهما في المملكة المتحدة.[77] والعلاقة بين Riot.im و Matrix لها آثار ملحوظة على فهم المتطرفين موضوع الخصوصية والأمن على المنصة. أولاً، كثيرًا ما يفضل مستخدمو Riot.im المتطرفون استضافة اتصالاتهم على خوادم Matrix العامة الافتراضية، بدلاً من إنشاء خوادم لامركزية خاصة بهم وإدارتها.[78] وهذا يعني أن اتصالاتهم تشملها شروط خدمة Matrix وتخضع لقواعد تنظيمية صارمة بشأن المحتوى المتطرف عبر الإنترنت في المملكة المتحدة. وتحظر شروط خدمة Matrix استخدام الخدمة "لأية أغراض غير قانونية أو لدعم أنشطة غير قانونية بموجب قانون المملكة المتحدة/الاتحاد الأوروبي"، بما في ذلك المحتوى الإرهابي.[79] وبالتالي،

65 "Features". بلا تاريخ. تطبيق Riot.im. تم الوصول في 1 أبريل 2020. https://about.riot.im/features.
66 المرجع نفسه.
67 المرجع نفسه.
68 Flashpoint, "Jihadists Presence Online Decentralizes After Telegram Ban"؛
Gluck, "Islamic State Adjusts Strategy to Remain on Telegram".
69 المرجع نفسه.
70 King, Peter. 2019. "Islamic State Group's Experiments with the Decentralized Web." Europol. https://www.europol.europa.eu/publications-documents/islamic-state-group%E2%80%99s-experiments-decentralised-web.
71 Communication with Jon Lewis, Program on Extremism، 1 أبريل 2020.
72 Bodo, Lorand. 2018. "Decentralised Terrorism: The Next Big Step for the so-Called Islamic State (IS)?" VOX – Pol. 12 ديسمبر 2018. https://www.voxpol.eu/decentralised-terrorism-the-next-big-step-for-the-so-called-islamic-state-is/.
73 Riot.im, "Features".
74 المرجع نفسه.
75 المرجع نفسه.
76 المرجع نفسه.
77 "Privacy Notice". بلا تاريخ. تطبيق Riot.im. تم الوصول في 1 أبريل 2020. https://riot.im/privacy.
78 King, "Islamic State Group's Experiments with the Decentralized Web".
79 Riot.im, "Privacy Notice".

تُزيل الشركة المحتوى والحسابات المتطرفة عن منصاتها بانتظام. وعندما تستضيف الجماعات المتطرفة محتوى على خوادم لامركزية تابعة للغير، فغالبًا ما تجد نفسها أمام خدمة رديئة وجهود إزالة مستقلة يقوم بها أصحاب المنصات الصغيرة.[80] وحتى الآن، لم يأخذ بزمام المبادرة واستضافة دردشات Riot.im على خوادم ذاتية الإدارة إلا عدد قليل من المتطرفين.[81]

منصة Rocket.Chat

Rocket.Chat عبارة عن منصة لامركزية للمراسلة الفورية عبر الإنترنت توفر لمستخدميها إمكانية استضافة المحتوى والاتصالات على خوادمهم الخاصة أو تخزين المواد على خادم Rocket.Chat العام.[82] والجدير بالذكر أن وسائل تنظيم داعش الإعلامية المركزية جربت، في ديسمبر 2018، إدارة خادم اتصالاتها الخاص على منصة Rocket.Chat، وهي من أولى محاولات الجهاديين الاستفادة الكاملة من منصات الويب اللامركزية.[83] واستضافت وكالة أنباء ناشر التابعة لتنظيم داعش العديد من قنوات Rocket.Chat على خادم يسمى Techhaven، والذي ذُكِر في دليل مستخدمه أنه مصمم لتوفير "منتدىً مفتوحًا للنقاش والخصوصية الرقمية والابتكار للمستخدمين المضطهدين في مناطق النزاع الذين تستهدفهم بسبب معتقداتهم الأنظمةُ الاستبداديةُ في الغرب."[84] ومنذ ذلك الحين، يعكف تنظيم داعش والجماعات الجهادية الأخرى، بما فيها القاعدة، على إنشاء قنوات ومجموعات على منصة Rocket.Chat.[85]

ومنصة Rocket.Chat، بخلاف غيرها من المنصات التي تناولها هذا التقرير، تشبه Riot.im إلى حد كبير من حيث أنهما منصتان للمراسلة صُمِّمتا في البداية للتعاون في تسيير العمل المكتبي الذي يوفر للمستخدمين إمكانية اختيار الخوادم المدارة مركزيًا أو الخوادم اللامركزية التي يديرها المستخدمون.[86] والأسهل إنشاء الخادم وإدارته على Rocket.Chat وليس Riot.im. وإنشاء حساب على خادم Rocket.Chat العام أو الاشتراك في خادم مستضاف استضافة خاصة يتطلب اسمَ مستخدم وكلمةَ مرور وبريدًا إلكترونيًا.[87] وبمجرد إنشاء الحساب، يستطيع المستخدمون بدء الدردشة مباشرةً مع مستخدمين آخرين أو إنشاء قنوات عامة أو قنوات بالدعوة فقط. وتتضمن المنصة أيضًا ميزات فريدة أخرى متعددة من المحتمل أن تكون جذابة للجماعات المتطرفة، ومنها الترجمة الآلية للمشاركات من لغة إلى أخرى.[88]

ويُعد خيار استضافة الخوادم اللامركزية معضلةً تواجه الجماعات المتطرفة. فإذا فضلوا استضافة اتصالات Rocket.Chat على خادم الشركة المركزي، فإن الشركة يمكنها إما إزالة القنوات التي تروج التطرف وفقًا لقواعد سلوك المستخدم أو، في حالة وجود أسباب ملزمة، أن تصبح الشركة "مطالبة بالإفصاح عن بياناتك الشخصية إذا لزم الأمر بموجب القانون أو استجابة لطلبات قانونية من السلطات العامة."[89] وقد يستغرق اختيار استضافة الاتصالات على خادم لامركزي وقتًا طويلاً. ويحتاج إلى خبرة تقنية، وقد يُعرِّض الجماعات المتطرفة لمشكلات أخرى.[90] وبعد ثلاثة أشهر من إنشاء وكالة ناشر الإخبارية قنواتها على خادم Techhaven، تم استهداف الشركة المضيفة بهجمات موزعة رفضت الخدمة وجعلت معظم قنواتهم على Rocket.Chat غير صالحة للعمل.[91] وإنشاء خادم مخصص لاستضافة الدعاية المتطرفة قد يعرِّض الخادم للاستهداف الرقمي. وفي حالة حدوث الخلل المنشود، قد تضطر الجماعات المتطرفة على المنصات اللامركزية مثل Rocket.Chat إلى القفز من خادم إلى آخر، ما يقلل فائدة المنصة كقاعدة ثابتة للدعاية.

---

80 King, "Islamic State Group's Experiments with the Decentralized Web".
81 المرجع نفسه؛ Bodo, "Decentralized Terrorism".
82 "Rocket.Chat". بلا تاريخ. Rocket.Chat. تم الوصول في 1 أبريل 2020. https://rocket.chat/.
83 "Europol Disrupts IS Propaganda Machine". 2019. BBC News. 25 نوفمبر 2019، sec. Middle East. https://www.bbc.com/news/world-middle-east-50545816.
84 King, "Islamic State Group's Experiments with the Decentralized Web".
85 Flashpoint, "Jihadists Presence Online Decentralizes After Telegram Ban".
86 Rocket.Chat, "Rocket.Chat".
87 المرجع نفسه.
88 المرجع نفسه.
89 "Rocket.Chat Privacy Policy". بلا تاريخ. Rocket.Chat. تم الوصول في 1 أبريل 2020. https://rocket.chat/privacy.
90 King, "Islamic State Group's Experiments with the Decentralized Web".
91 المرجع نفسه.

برنامج TamTam

TamTam عبارة عن برنامج للمراسلة الفورية عبر الإنترنت تديره مجموعة Mail.ru، وهي الشركة الروسية التي تمتلك الحصة الأكبر من الإنترنت الناطق بالروسية وتشغل أيضًا منصتيْ وسائل التواصل الاجتماعي الشهيرتين Vkontakte و Odnoklassniki.[92] وبرنامج TamTam متطابق تقريبًا من الناحية الهيكلية مع تليغرام من حيث مجموعة ميزاته. ويوفر دردشات وقنوات عامة وقنوات خاصة وخيارات دردشة جماعية.[93] والتشابه بين تليغرام و TamTam مقصود. وأنشأت مجموعة Mail.ru برنامج TamTam كبديل لتليغرام خلال الجهود المستمرة التي تبذلها الحكومة الروسية لحظر عناوين IP تليغرام عن الإنترنت الروسي.[94] وتتمتع مجموعة Mail.ru بعلاقات وثيقة مع الحكومة الروسية، وهناك مزاعم أنها أكثر استعدادًا من نظيرتها لتلبية طلبات جهات تنفيذ القانون الروسية الحصول على بيانات المستخدمين.[95]

وأنشأ أنصار داعش عددًا كبيرًا من القنوات والمجموعات على TamTam عقب الإجراء المنسق الذي اتخذه يوروبول على تليغرام في ديسمبر 2019.[96] وتحركت شركة TamTam بسرعة لمواجهة زيادة المحتوى المرتبط بداعش.[97] وصرح متحدث باسم الشركة لـ Vice News بأن TamTam "تعارض بشدة وجود أي نوع من محتوى المنظمات الإرهابية على منصتنا" ودعا المستخدمين إلى الإبلاغ عن أي محتوى أو حسابات تروج للجماعات الإرهابية.[98] وبعد حملة تطهير قامت بها TamTam، أخذت الجماعات الجهادية تحذر متابعيها من استخدام المنصة.[99] على سبيل المثال، في فبراير 2020، نشرت مجموعة من أنصار تنظيم داعش الناطقين بالإنجليزية اسمها "أسود التوحيد" على موقع Rocket.Chat أن "الحكومة الروسية يمكنها الوصول إلى جميع حسابات TamTam ... احم نفسك بإزالة TamTam من هاتفك أو جهاز الكمبيوتر. استخدم تطبيقات آمنة مثل Riot و Rocket.Chat وتليغرام".[100]

يطلب TamTam من المستخدمين اتباع نفس الإجراءات مثل تليغرام لإنشاء حساب والوصول إلى المحتوى. ويوفر نفس مجموعة الميزات مثل تليغرام، بما في ذلك خيارات الدردشات واحد إلى واحد وقنوات واحد إلى متعددين ومحادثات جماعية كبيرة.[101] ويستطيع المستخدمون إتاحة الدردشات والقنوات للجمهور أو تخصيص إمكانية الوصول إليها بالدعوة فقط.[102] حتى إن أوجه تشابه TamTam مع تليغرام تمتد إلى اسم نطاقها أيضًا. ويتم الوصول إلى ارتباطات تليغرام التشعبية المختصرة من خلال اسم النطاق t.me؛ أما TamTam فيستخدم tt.me.[103] وتروج الشركة بنشاط لقابلية تشغيلها البيني مع تليغرام في السوق الروسية بالإعلان صراحة عن مدى تشابهها مع تليغرام على قنوات تليغرام الروسية الشهيرة.[104]

ويكمن الاختلاف الرئيسي بين تليغرام و TamTam في موضوع الخصوصية والأمان. وشركة TamTam مسجلة في الاتحاد الروسي وسياسة بياناتها "تُعالَج وفقًا لقوانين الاتحاد الروسي."[105] وهذا يعني أن TamTam، على عكس تليغرام، تحرص على الالتزام بالقانون الروسي الذي يُلزم مقدمي الخدمات بمنح إمكانية الوصول السري لخدمة الأمن الفيدرالية (FSB)، وهي وكالة إنفاذ القانون الرئيسية في الاتحاد الروسي.[106] وتشير إلى إنها تقوم بالتشفير، ولكن يعتقد الخبراء أنها ربما سلمت نسخًا من مفاتيح

92 "Some Messenger Called 'TamTam' Is Trying to Replace Telegram in Russia. What the Heck Is It?" 2018. Meduza. 17 أبريل 2018. https://meduza.io/en/feature/2018/04/17/some-messenger-called-tamtam-is-trying-to-replace-telegram-in-russia-what-the-heck-is-it.
93 المرجع نفسه.
94 المرجع نفسه.
95 المرجع نفسه.
96 Flashpoint, "Jihadists Presence Online Decentralizes After Telegram Ban"; Gluck, "Islamic State Adjusts Strategy to Remain on Telegram"; Amarasingam, "Telegram Deplatforming ISIS Has Given Them Something to Fight For"; Bloom, "No Place to Hide, No Place to Post."
97 المرجع نفسه.
98 Gilbert, David. 2019. "The Russian Social Network Letting ISIS Back Online." Vice. 3 ديسمبر 2019. https://www.vice.com/en_us/article/d3ane7/islamic-state-cant-find-an-online-home-so-they-might-build-their-own-app.
99 "Pro-ISIS Outlet Lists 'Safe' Messaging Apps, Advises Against Using Chinese, Russian Apps." 2020. MEMRI. 18 مارس 2020. https://www.memri.org/cjlab/pro-isis-outlet-lists-safe-messaging-apps-advises-against-using-chinese-russian-apps.
100 المرجع نفسه.
101 "About TamTam". بلا عنوان. TamTam. تم الوصول في 1 أبريل 2020. https://about.tamtam.chat/en/index.html.
102 المرجع نفسه.
103 Meduza, "Some Messenger Called 'TamTam' Is Trying to Replace Telegram in Russia."
104 المرجع نفسه.
105 "TamTam Messenger Confidentiality Policy". بلا تاريخ. TamTam. تم الوصول في 1 أبريل 2020. https://about.tamtam.chat/en/policy/index.html.
106 المرجع نفسه.

تشفير TamTam إلى خدمة FSB.[107] وتحظر اتفاقية ترخيص TamTam صراحةً على المستخدمين "[نشر] التطرف أو الإرهاب أو التحريض على [إثارة] العداء على أساس الهوية العرقية أو الاثنية أو القومية" أو نشر "معلومات ذات طبيعة متطرفة."[108] ومن المنطقي أن نفترض أن أنصار داعش فيما يحاولون استغلال TamTam في أعقاب أيام إجراءات إحالة اليوروبول 2019، اختاروا TamTam لتشابهه مع تليغرام في مقابل ميزات الخصوصية والأمان لديه.

شكل 1: مقارنة بين منصات المراسلة الفورية النصية التي تستخدمها الجماعات المتطرفة

المنصة	الاستخدام المتطرف	دولة التسجيل	مجموعة الميزات	الأمان	السياسات/البيئة التنظيمية
تليغرام	جهادي (داعش، القاعدة)، يمين متطرف	جزر فيرجن البريطانية/ الإمارات العربية المتحدة	• دردشات واحد إلى واحد • دردشات جماعية • دردشات عامة وخاصة	• تشفير من النهاية إلى النهاية لدردشات واحد إلى واحد • الإتلاف الذاتي للحساب/للبيانات	• سوف تزيل المحتوى العام "الإرهابي" (البوتات والقنوات العامة) • بأمر المحكمة، سوف تقدم معلومات المستخدم لجهات إنفاذ القانون في القضايا المتعلقة بالإرهاب
*BCM	جهادي (داعش)	جزر فيرجن البريطانية	• دردشات واحد إلى واحد • دردشات جماعية	• تشفير من النهاية إلى النهاية • الإتلاف الذاتي للحساب/للبيانات • خيار الخادم اللامركزي	• لا توجد سياسة معروفة بشأن إزالة المحتوى المتطرف أو إدارته • عدم إفصاح الغير عن بيانات المستخدم لتطبيق القانون
**Gab Chat	يمين متطرف	الولايات المتحدة الأمريكية	• دردشات واحد إلى واحد • دردشات جماعية	• تشفير من النهاية إلى النهاية على الجهاز • حذف الرسالة على الخادم بعد 30 يومًا	• الكلام "المسيء" و "البغيض" ليس سببًا لإزالة المحتوى، "المحتوى والنشاط غير القانوني" فقط • سوف تتعاون مع حكومة الولايات المتحدة بشأن المطالبة القانونية ببيانات المستخدم أثناء التحقيقات، وليس مع الحكومات الأخرى أو الغير
Hoop Messenger	جهادي (داعش، القاعدة)	كندا	• دردشات واحد إلى واحد • دردشات جماعية • قنوات عامة وخاصة	• تشفير من النهاية إلى النهاية لجميع الدردشات والملفات في نظام "Vault" المحمي بكلمة مرور • حذف الحسابات والمحتوى من Vault عن بُعد	• الشركة "سوف تزيل المحتوى الذي نرى، حسب تقديرنا، أنه غير قانوني أو فاحش أو مسيء أو تهديدي أو تشهيري أو افترائي أو غير مرغوب لسبب آخر"

107 المرجع نفسه.
108 "TamTam Messenger End User License Agreement". بلا تاريخ. TamTam. تم الوصول في 1 أبريل 2020. https://about.tamtam.chat/en/license/index.html.

المنصة	الاستخدام المتطرف	دولة التسجيل	مجموعة الميزات	الأمان	السياسات/البيئة التنظيمية
Riot.im	جهادي (داعش، القاعدة)، يمين متطرف	المملكة المتحدة	• دردشات واحد إلى واحد • دردشات جماعية	• قيام المستخدم بتفعيل التشفير من النهاية إلى النهاية • خيار الخادم اللامركزي	• تستطيع الشركة إزالة المحتوى عن الخوادم العامة التي تدعم "أية أغراض غير قانونية أو الداعمة لأنشطة غير قانونية بموجب قانون المملكة المتحدة/الاتحاد الأوروبي"
Rocket.Chat	جهادي (داعش، القاعدة)	الولايات المتحدة الأمريكية/ البرازيل	• دردشات واحد إلى واحد • دردشات جماعية • قنوات عامة وخاصة	• قيام المستخدم بتفعيل التشفير من النهاية إلى النهاية • خيار الخادم اللامركزي	• الشركة "مطالبة بالإفصاح عن بياناتك الشخصية إذا لزم الأمر بموجب القانون أو استجابة لطلبات قانونية من السلطات العامة"
TamTam	جهادي (داعش، القاعدة)	الاتحاد الروسي	• دردشات واحد إلى واحد • دردشات جماعية • قنوات عامة وخاصة	• "التشفير" (بروتوكول غير واضح)	• تحظر الشركة نشر "التطرف أو الإرهاب أو التحريض على [إثارة] العداء على أساس الهوية العرقية أو الاثنية أو القومية" أو نشر "معلومات ذات طبيعة متطرفة" • "يلزم معالجة بيانات المستخدمين وفقًا لقوانين الاتحاد الروسي"، ما يتطلب الإفصاح الإجباري عن المعلومات ومفاتيح التشفير لتطبيق القانون الروسي

* توقفت الخدمة، فبراير 2020
** في مرحلة التجريب حاليًا

4 التحليل: منحنى تبني المتطرفين تطبيقات المراسلة الفورية النصية

تُعد تجارب المتطرفين مع خدمات المراسلة الفورية النصية عبر الإنترنت جانبًا مهمًا من جهودهم نحو تبني التكنولوجيا الناشئة. وبعد الصعوبات التي واجهت المتطرفين على تليغرام، فإن تبنيهم تطبيقات المراسلة الثانوية يتبع عمومًا ما أشار إليه كل من Daveed Gartenstein-Ross و Matt Shear و David Jones باسم "منحنى تبني التكنولوجيا من قبل الجهات الفاعلة العنيفة غير الحكومية (VNSA)."[109] ويقوم المتطرفون بمحاولات (فاشلة عادة) لتسخير التكنولوجيا الناشئة، في أولى مراحل تبنيها المبكر.[110] وفيما يمارسون التكنولوجيا، يبدأون في تحسين قدرتهم على استخدامها، بينما تُطرح منتجات جديدة في السوق تساعدهم في مساعيهم.[111] وبعد ممارستها، قد تتوصل الجماعات المتطرفة إلى وسيلة مبتكرة – كأن يقعوا على طريقة معينة لاستخدام التكنولوجيا تعزز استراتيجياتهم كثيرًا.[112] ولكن تواجه الجماعات المتطرفة حتمًا منافسة تتمثل في استجابة الحكومات ومقدمي الخدمات لها.[113] وهذه المنافسة الكبيرة يمكنها إعادة تحريك منحنى التبني، وهذه المرة لبدائل التكنولوجيا الأصلية حيث تضطر الجماعات المتطرفة إلى تجربة التبني المبكر للتقنيات الجديدة.[114]

يمكننا القول إن التقدم الذي حققه المتطرفون في فترة 2015–2017 في استخدام تليغرام ينتقل إلى مرحلة المنافسة. وخلال العام الماضي، بدأت تليغرام، بالتعاون مع جهات حكومية، تناهض استخدام المتطرفين المنصة بصورة ملحوظة. وهذا ما دفع المتطرفين بمختلف طوائفهم إلى إعادة بدء مرحلة التبني المبكر لاستخدام العديد من بدائل تليغرام.[115] وباستخدام منحنى تبني التكنولوجيا من قبل الجهات الفاعلة العنيفة غير الحكومية (VNSA) كدليل، نجد أن معظم الجهود الحالية التي تبذلها الجماعات المتطرفة لإيجاد بديل مستدام وآمن لتليغرام تبوء بالفشل. ولكن، فيما يتعلق بتبني منصات التواصل الاجتماعي الجديدة، تتمتع الجماعات المتطرفة بسجل حافل بسرعة التعلم التنظيمي.[116] ومع ظهور منصات المراسلة الفورية التي يتزايد استقرارها وتقدم ميزات جديدة لتعزيز الخصوصية والأمان، يتساءل المتطرفون، الذين ينتقلون من تليغرام إلى برنامج ثانوي للمراسلة الفورية، "متى" و "ماذا"، وليس "لو".

من المحتمل أن تبتعد الجماعات المتطرفة المختلفة عن تليغرام في أوقات مختلفة، لأنها تواجه حاليًا منافسةً متباينةً على المنصة. وتركز التدابير التي تتخذها الشركة والحكومات ضد المتطرفين على تليغرام، من عمليات إزالة المحتوى والحسابات إلى جهود المراقبة، على أنصار داعش عمومًا.[117] وفي الوقت نفسه، يواجه أنصار الجماعات

109 Gartenstein-Ross, Daveed, Matt Shear and David Jones. 2019. "Virtual Plotters. Drones. Weaponized AI?: Violent Non-State Actors as Deadly Early Adopters." Washington, D.C.: Valens Global. http://valensglobal.com/virtual-plotters-drones-weaponized-ai-violent-non-state-actors-as-deadly-early-adopters/.

110 المرجع نفسه.

111 المرجع نفسه.

112 المرجع نفسه.

113 المرجع نفسه.

114 المرجع نفسه.

115 Flashpoint, "Jihadists Presence Online Decentralizes After Telegram Ban"; Gluck, "Islamic State Adjusts Strategy to Remain on Telegram"; Amarasingam, "Telegram Deplatforming ISIS Has Given Them Something to Fight For"; Bloom, "No Place to Hide, No Place to Post".

116 Shapiro, Jacob N. 2015. The Terrorists Dilemma: Managing Violent Covert Organizations. Reprint edition. Princeton University Press; Kenney, Michael. 2010. "Beyond the Internet: Mētis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists." Terrorism and Political Violence 22 (2): 177–97. https://doi.org/10.1080/09546550903554760; Gartenstein-Ross et al., "Virtual Plotters. Drones. Weaponized AI?"; Alexander, "Digital Decay."

117 Amarasingam, "A View from the CT Foxhole"; Conway, Maura, Moign Khawaja, Suraj Lakhani, Jeremy Reffin, Andrew Robertson and David Weir. 2019. "Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts." Studies in Conflict & Terrorism 42 (1–2): 141–60. https://doi.org/10.1080/1057610X.2018.1513984; Conway, Maura, Ryan Scrivens and Logan Macnair. 2019. "Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends." The Hague, Netherlands: International Centre for Counter-terrorism. https://icct.nl/wp-content/uploads/2019/11/Right-Wing-Extremists-Persistent-Online-Presence.pdf.

المتطرفة الأخرى، بما فيها المتطرفون اليمينيون المتشددون والجماعات الجهادية الأخرى، معارضةً محدودةً، وبالتالي ليس هناك ما يحدوهم بقوة على ترك المنصة.[118] ولهذا السبب، نُرجح أن يبذل أنصار داعش المزيد من الجهود لتجربة منصات المراسلة الفورية الناشئة كبدائل عامة لتليغرام. ولكن إذا بدأت تليغرام حملات قمع كبيرة على أنواع أخرى من الأنشطة المتطرفة على منصتها، فقد تحذو حذوها مجموعة كبيرة من الجهاديين والجماعات اليمينية المتطرفة.

وإذا أجرينا تقييمًا أوليًا قائمًا على المنصات المذكورة أعلاه، ظهرت بعض الميزات التي قد تبحث عنها الجماعات المتطرفة من أجل تبني بدائل تليغرام. وتظهر أوجه التشابه والاتجاهات الملحوظة في هذه المجموعة من تطبيقات المراسلة الفورية التي تبنتها الجماعات المتطرفة في أعقاب المنافسة المتزايدة على تليغرام. أولاً، يوفر العديد منها خيارات ومزايا للاتصال مشابهة جدًا لتليغرام. وليس من قبيل الصدفة أن كانت TamTam من أوائل المنصات التي عزز عليها أنصار داعش أتباعهم في الفترة التي أعقبت أيام إجراءات إحالة اليوروبول.[119] وهذا التطبيق عبارة عن نسخة شبه كربونية من تليغرام، بل وهكذا يُروَّج له. ومع أن ميزات الأمان والخصوصية التي يقدمها لا تكاد تُذكر، سرعان ما اجتذب مستخدمي تليغرام المتطرفين لتشابهه مع منصتها. وفي مستهل مراحل العثور على بديل تليغرام، كان التشابه مع تليغرام يُعد ميزة للجماعات المتطرفة لسرعة تكيف أنصارها مع المنصة الجديد، ما يضمن سهولة استخدامها والتعامل معها.

ويتضح من التحليل أعلاه أيضًا إقبال الجماعات المتطرفة على تجريب منصات المراسلة الفورية التي توفر خوادم لامركزية وإمكانية تخزين البيانات. ويبدو أن معظم الجماعات لم تستفد استفادة كاملة، حتى الآن، من خيار إلغاء مركزية تخزين البيانات أثناء استخدام منصات مثل BCM أو Riot.im أو Rocket.Chat.[120] وقد تستغرق إدارة الخوادم المستقلة لهذه المنصات وقتًا طويلاً، وتستهلك الكثير من الموارد – هذا ما توصلت إليه وكالة ناشر الإخبارية عندما حاولت إنشاء خادم Rocket.Chat لامركزي للدردشة من أجل قنواتها الدعائية - وتحديد أهداف إضافية للحكومات والمنافسين والقراصنة المستقلين.[121] وتواجه عمليات التعميم الأولية لهذه المنصات وجهود المتطرفين البدائية لاستغلالها خللاً ورفضًا للخدمة وغيرها من المشكلات التكنولوجية. ولكن المنصات الجديدة، مثل ZeroNet و Matrix وغيرهما، تجعل استضافة الخوادم اللامركزية أسهل بكثير للمستهلكين، ما يضع هذه المنصات حتمًا في متناول الجماعات المتطرفة أكثر من غيرها.[122]

ومع ذلك، قد تكون منصة المراسلة الفورية القائمة على شبكة ويب لامركزية مرشحةً جيدةً كتطبيق بديل عن تليغرام، لاسيما إذا أصبحت متاحة بسهولة للمتطرفين وسهلة الاستخدام. وكتب Lorand Bodo قائلاً "فيما يبدو أن شبكة الويب اللامركزية هي الخطوة المنطقية التالية لداعش ولغيرها من المتطرفين (العنيفين) عبر الإنترنت الذين يحاولون الإفلات من السلطات وعمليات الإزالة."[123] والدافع لتبني منصات الويب اللامركزية بسيط: يواجه المتطرفون عبر الإنترنت تهديدات من الحكومات التي تحاول مراقبة الإرهابيين المحتملين والتعرف عليهم والتصدي لهم ومن مقدمي الخدمات التكنولوجية الذين يحاولون القضاء على وجود الدعاية المتطرفة على منصاتهم.[124] وأصبح المتطرفون الآن، من خلال تليغرام والخدمات الأخرى، بارعين في الاستفادة من الخدمات التي تعظم الخصوصية مثل التشفير من النهاية إلى النهاية، لكنهم يواجهون معركة شاقة في الحفاظ على قوة الشبكة على هذه المنصات.[125] وإذا تمكّنت هذه الجماعات من تخزين البيانات على خوادمها الخاصة، فهذا قد يخفف في الواقع تأثير جهود إزالة المحتوى التي تقوم بها شركات التكنولوجيا بإنشاء شبكة تخزين مستقلة لامركزية خارج نطاق مقدمي الخدمات.[126]

---

118 Amarasingam, "Telegram Deplatforming ISIS Has Given Them Something to Fight For".
119 King, "Islamic State Group's Experiments with the Decentralized Web"; Bodo, "Decentralized Terrorism".
120 المرجع نفسه.
121 المرجع نفسه.
122 المرجع نفسه.
123 Bodo, "Decentralized Terrorism".
124 المرجع نفسه.
125 المرجع نفسه.
126 المرجع نفسه.

5 التوصيات: نحو نهج يركز على الميزات عند التعامل مع التطرف عبر الإنترنت

إن انتشار برامج المراسلة المشابهة لتليغرام والتطبيقات اللامركزية الأخرى داخل تطبيقات الدردشة التي استغلها المتطرفون عقب احتدام المنافسة على تليغرام يؤكد أن تبني هذه التطبيقات مشروط بالميزات التي تقدمها. وفي المقابل، يتعين أن تبتعد سياسة مكافحة التطرف عبر الإنترنت عن التركيز على منصات أو تطبيقات بعينها، وأن تتبني، بدلاً من ذلك، نهجًا يركز على الميزات عند التعامل مع استغلال المتطرفين تقنيات الاتصالات الرقمية. وفيما ينصب اهتمام الباحثين وصانعي السياسات على عدد محدد من منصات "المشكلات" – في السنوات الأخيرة، تويتر وتليغرام – يتجاهل النظامَ الإيكولوجي للاتصالات المتطرفة عبر الإنترنت على نطاق أوسع.[127] وتؤدي هذه الديناميكية دورًا في غارات الإجراءات المستهدفة عبر الإنترنت مثل أيام إجراءات الإحالة لليوروبول التي دفعت عددًا من صانعي السياسات إلى وضع أطر لإزالة المحتوى على منصات معينة باعتبارها انتصارات ساحقة على التطرف عبر الإنترنت. وتوضح هذه الورقة أن اللامركزية المترتبة على استخدام المنصات يمكنها الإفلات من الآثار الإيجابية لهذه العمليات.[128]

وقد تستفيد جهود مكافحة التطرف عبر الإنترنت، عمومًا، من أي نهج يرتكز على الميزات بمطابقة الاستجابات السياسية مع الطرق التي يصور بها المتطرفون استخدامهم الإنترنت. وإذا ركز مقدمو هذه الخدمات على مكافحة الاستغلال المتطرف للميزات وليس المنصات لاستطاعوا العثور بسهولة على شركات مماثلة لتبادل الاستجابات والوسائل المبتكرة. وتشير البيانات المستمدة من دراسات متعددة أجريت على منصات معينة إلى أن إقبال المتطرفين على هذه التطبيقات يرجع إلى ما تقدمه من ميزات وليس بسبب علامتها التجارية أو شرعيتها.[129]

ويميل صانعو السياسات الأوروبيون والأمريكيون ذوو الصلاحيات التنظيمية إلى تحديد منصات معينة واستهدافها بالقيود التنظيمية والمثبطات المستهدفة والإنذارات بهدف التصدي لاستغلال المتطرفين للإنترنت. وقد تكون هذه الإجراءات ضرورية في بعض الحالات. ولسوء الحظ، بعض المنصات لها سجلات تتبع سيئة للغاية فيما يتعلق بالتطرف عبر الإنترنت لعدم التزامها بشروط الخدمة، أو لوجود ثغرات عميقة في إمكاناتها، أو لسوء بيئاتها التنظيمية، أو لتحيزها لمجموعات متطرفة معينة تعرقل أداءها. ومن الضروري تحديد هذه المنصات وإخضاعها لقواعد تنظيمية. ومع ذلك، ينتشر الاستغلال المتطرف على المنصات التي تجذب المتطرفين بميزاتها أو بقاعدتها الجماهيرية العريضة، بالرغم من الجهود التي تبذلها بحسن نية لإدارة المحتوى و/أو إزالته. ولتقييم مدى استغلال المتطرفين لإمكانات معينة في مختلف المنصات، قد يستعين صانعو السياسات بنهج قائم على الميزات للتمييز بين المنصات التي تعاني من أمور تتعلق بحوكمة المحتوى وإدارته، التي قد تتعامل جيدًا مع الضغوط، والمنصات التي تجذب المتطرفين بميزاتها بكل بساطة، وما سواها.

وبالنسبة للهيئات المعنية بمكافحة التطرف عبر الإنترنت، مثل منتدى الإنترنت العالمي لمكافحة الإرهاب (GIFCT)، قد يساعد تجميع المنصات المتماثلة الشركاءَ على تصميم أهداف محورية وشاملة لمكافحة التطرف وفقًا لميزات محددة مشتركة

127 Alexander, Audrey, and Bill Braniff. 2018. "Marginalizing Violent Extremism Online." Lawfare. 21 يناير 2018. https://www.lawfareblog.com/marginalizing-violent-extremism-online;
Fisher, Ali, Prucha, Nico and Emily Winterbotham. 2019. "Mapping the Jihadist Information Ecosystem: Towards the Next Generation of Disruption Capability." Global Research Network on Terrorism and Technology: Paper No. 6، يوليو 2020. https://rusi.org/sites/default/files/20190716_grntt_paper_06.pdf.

128 Alexander and Braniff, "Marginalizing Violent Extremism Online".

129 المرجع نفسه.

بين هذه المنصات. ويرى علي فيشر ونيكو بروشا وإميلي وينتربوذام أن "التركيز على نموذج الاتصال المتعدد المنصات بدلاً من المنصات الفردية هو مفتاح التطوير المستقبلي لنهج من الجيل التالي للتعامل مع أي خلل في الإنترنت."[130] ويمكننا تعزيز التعاون والابتكار عن طريق تبادل أفضل الممارسات وطرق التعامل والأفكار بين مختلف المنصات التي تقدم ميزات متماثلة، مثل منصات تبادل الملفات أو برامج المراسلة الفورية أو مواقع التواصل الاجتماعي. وهذا يؤدي إلى تعزيز وسائل تبادل المعلومات الحالية، مثل قواعد البيانات الخاصة بتبادل العناوين الإلكترونية، عن طريق تمكين المنصات المختلفة من تتبع مسارات انتقال المحتوى المتطرف من منصة إلى أخرى.[131]

وأخيرًا، بل والأهم من ذلك أن تعزيز التعاون بين المنصات ذات الميزات المتماثلة يُعد بمثابة نظام إنذار مبكر للمتطرفين المتنقلين بين المنصات. وكمثال على ذلك، فإن منصات المراسلة الفورية التي تنتمي لتجمع معني بتبادل المعلومات مع غيرها من المنصات تخطر الآخرين عبر قنواتها المباشرة بما تعتزم اتخاذه من إجراءات صارمة لإزالة المحتوى والشبكات المتطرفة عن منصاتها. وتستطيع منصات المراسلة الفورية الأخرى، التي تتلقى إخطارًا مسبقًا بأن المتطرفين قد يفكرون في التحول إلى خدماتهم نتيجة لذلك، إعداد استجاباتها استباقيًا. وقدرة مقدمي الخدمات على عرقلة تبني المتطرفين منصات جديدة في مرحلة الممارسة المبكرة يمكنها أن تمنع المتطرفين من إنشاء نقاط انطلاق بسهولة ويسر على منصات جديدة.

وفيما يتوسع منتدى الإنترنت العالمي لمكافحة الإرهاب (GIFCT) في عضويته لتشمل شركات جديدة في السنوات المقبلة، يجب أن يضع في الاعتبار الجمع بين السبل الحالية واسعة النطاق للتعاون مع مجموعات عمل محدودة تجمع مقدمي الخدمات معًا في فئات محددة. وبينما توضح هذه الورقة فوائد هذا النموذج التعاوني لمنصات المراسلة الفورية، نحتاج إلى المزيد من البحوث والتجارب لتحديد ما إذا كان هناك أنواع أخرى من مقدمي الخدمات، مثل وسائل التواصل الاجتماعي أو تبادل الملفات أو التجارة الإلكترونية، يمكنها الاستفادة من هذه التجمعات المعنية بالميزات في إطار منتدى الإنترنت العالمي لمكافحة الإرهاب (GIFCT). ونحتاج الأخذ بزمام هذه المبادرة لتمكين هذا النهج داخل منتدى الإنترنت العالمي لمكافحة الإرهاب (GIFCT) من توجيه صانعي السياسات والباحثين نحو إجراء تقييم دقيق لدور الميزات في تعديل ميول المتطرفين، وتحديد طريقة تعاملها مع مختلف السياسات وإجراء الأبحاث اللازمة لاستيعاب مساحات أوسع من النظام الإيكولوجي المتطرف عبر الإنترنت. وباختصار، تستطيع شركات التكنولوجيا وصانعي السياسات والممارسين والباحثين أن يستعينوا بهذا النموذج القائم على الميزات في تقويم منحنى استغلال المتطرفين لتكنولوجيات الاتصالات الرقمية.

130 Fisher et al. "Mapping the Jihadist Information Ecosystem".

131 المرجع نفسه.

المشهد السياسي

كتب هذا القسم أرميدا شان ريج ولوسي توماس، وهما باحثتان مشاركتان في معهد السياسات في كينجز كوليدج لندن. ويلقي نظرة عامة على المشهد السياسي وعلاقته بهذا التقرير.

مقدمة

طالما كان استخدام الإنترنت وإساءة استخدامه من قبل الإرهابيين يشكلان تحديًا لصانعي السياسات وجهات تطبيق القانون وشركات التكنولوجيا على حد سواء. فهناك حالات عامة جدًا لسوء استخدام التكنولوجيا: البث المباشر للهجوم الإرهابي في نيوزيلندا على سبيل المثال. ولكن من المشكلات الأخرى المحتملة استخدام الإرهابيين أو المنظمات الإرهابية تطبيقات المراسلة الخاصة للتخطيط والتجنيد لصالح أنشطتهم. وازداد إقبال المنظمات الإرهابية على استخدام تطبيقات المراسلة المشفرة من النهاية إلى النهاية، وذلك على وجه التحديد لأنها توفر وسيلة اتصالات خاصة لا تستطيع وكالات إنفاذ القانون الوصول إليها بسهولة. وفي السنوات الأخيرة تعاظمت هذه المشكلة لدى تطبيق المراسلة تليغرام، وغيره من البدائل الأحدث، فيما يبحث الإرهابيون عن بدائل يتوارون خلفها من تطبيق القانون.

ويطرح هذا التقرير بعض التحديات الرئيسة التي تواجه حكومات الدول في التعامل مع تطبيقات المراسلة المشفرة من النهاية إلى النهاية. ومنها تسع دول يوضح تشريعاتها الرئيسية وأصحاب المصلحة فيها والتحديات التي تواجه صانعي السياسات عند تصديهم لإساءة استخدام تطبيقات المراسلة، فضلاً عن التحديات التي تواجه جهات إنفاذ القانون عند إجراء تحقيقاتها بسبب التشفير. وسوف يناقش التحديات التي يطرحها التحرك نحو منصات المراسلة اللامركزية والنُهج المُمكنة لحوكمتها.

تطبيقات المراسلة الفورية ومكافحة التطرف العنيف: مواجهة التحديات وتقييم التطورات الجديدة

كندا

تتسم استراتيجية الحكومة الكندية لمكافحة الإرهاب والراديكالية بالشمولية، وتضم أنشطة وكالات الاستخبارات والأمن التقليدية، ومشاركة المجتمع المدني، والمبادرات التعاونية مع أرباب الصناعة والشرطة المجتمعية. وتتخذ الاستراتيجية الكندية، حسب ما جاء في الاستراتيجية الكندية الوطنية لمكافحة راديكالية العنف، ثلاثة مسارات: صياغة رسائل مضادة مع المجتمع المدني، ودعم أبحاث مكافحة التطرف العنيف، وتعزيز الشراكة في المبادرات الدولية ومع شركات التكنولوجيا.[132]

ربما تكون استراتيجية كندا هي الأكثر تطورًا بين استراتيجيات الرسائل المضادة التي تركز على المجتمع المدني في جميع الولايات القضائية قيد المراجعة هنا. و Extreme Dialogue عبارة عن مبادرة للرسائل المضادة بين الحكومة الكندية ومعهد الحوار الاستراتيجي. وهذا المشروع يوفر موارد تعليمية للممارسين والشباب في إطار أفلام توضح التأثير السلبي للتطرف.[133] ويشهد المركز الكندي للمشاركة المجتمعية والوقاية

132 'National Strategy on Countering Radicalization to Violence,' Public Safety Canada. متاح: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-strtg-cntrng-rdclztn-vlnc/index-en.aspx#s7

133 انظر: https://extremedialogue.org/

من العنف عددًا من الفعاليات المجتمعية لمكافحة راديكالية العنف. ويعمل برنامج ReDirect، في كالغاري، على سبيل المثال، مع دائرة شرطة كالغاري وخدمات المجتمع والحي في مدينة كالغاري، بالإضافة إلى إدارات الخدمات الصحية والاجتماعية للتدخل في بدايات مراحل التطرف. ويستعين برنامج ReDirect بمجموعة من الاستراتيجيات، منها الإحالة والتعليم وتقديم المشورة، للباحثين عن طريقة للانشقاق عن جماعة متطرفة عنيفة.[134]

فيما يتعلق بدعم بحوث مكافحة التطرف العنيف، في عام 2019، كلفت كندا مبادرة Tech Against Terrorism الدولية التي ترعاها الأمم المتحدة وتعمل مع صناعة التكنولوجيا العالمية بتطوير منصة تحليلات المحتوى الإرهابي (TCAP)، وهي قاعدة بيانات محملة بمواد ومحتوى إرهابي تم التحقق منها مستقاة من مجموعات البيانات الحالية ومصادر مفتوحة.[135] وهذه المنصة لديها القدرة على العمل كمرفق تنبيه مباشر لمنصات الإنترنت الأصغر منها التي قد لا تكون لديها القدرة أو الموارد اللازمة للامتثال للجهود التنظيمية لإزالة المحتوى الضار والمتطرف.

وأخيرًا، تُعد كندا طرفًا في عددٍ من المبادرات الدولية والمشتركة بين القطاعات. وبعد الهجمات التي تعرض لها مسجد كرايستشيرش في مارس 2019، انضم رئيس الوزراء جاستن ترودو إلى دعوة كرايستشيرش للعمل، وهي عبارة عن تعهد مشترك بين الحكومات وصناعة التكنولوجيا "للقضاء على المحتوى المتطرف الإرهابي والعنيف على الإنترنت."[136] وفضلاً عن الرعاية المشتركة للتطويرات التقنية المطلوبة لتعقب المحتوى المتطرف وإزالته – مثل قاعدة بيانات هاشتاجات منتدى الإنترنت العالمي لمكافحة الإرهاب (GIFCT)[137] – تُلزم دعوة العمل هذه الحكومات بدعم الأطر وأنشطة بناء القدرات وتعزيز الوعي لمنع استخدام الخدمات عبر الإنترنت لنشر المحتوى الإرهابي والمتطرف العنيف.

المفوضية الأوروبية

تضم منظمة اليوروبول مقر المركز الأوروبي لمكافحة الإرهاب (ECTC) الذي أنشيء عقب هجوم عام 2015 على موظفي المجلة الساخرة شارلي إبدو في باريس، بناءً على مقترح ورد في جدول الأعمال الأوروبي المعني بالأمن للمفوضية الأوروبية. والهدف من المركز الأوروبي لمكافحة الإرهاب (ECTC) هو "تحسين تبادل المعلومات والدعم التشغيلي لمحققي الدول الأعضاء".[138] وفي عام 2015، أطلقت المفوضية أيضًا منتدى الاتحاد الأوروبي للإنترنت، الذي يجمع بين الحكومات واليوروبول وشركات التكنولوجيا والتواصل الاجتماعي لضمان إزالة المحتوى غير القانوني في أسرع وقت ممكن.[139]

وتدرك المفوضية الأوروبية أن المنظمات الإرهابية لا تستخدم وتسيء استخدام شركات التكنولوجيا الكبرى فحسب، وإنما المؤسسات الصغيرة التي تقدم "خدمات الاستضافة بمختلف أنواعها" أيضًا.[140] وثبت أن التشفير الآمن وإمكانية الوصول إلى البيانات الخاصة يمثلان تحديًا يواجه إنفاذ القانون أثناء التحقيقات.

---

134 انظر: http://redirect.cpsevents.ca/

135 تناولنا منصة تحليلات المحتوى الإرهابي (TCAP) أيضًا في قسم المشهد السياسي من تقرير الشبكة العالمية للتطرف والتكنولوجيا (GNET) عن "تحليل شفرة الكراهية: استخدام التحليل التجريبي للنصوص في تصنيف المحتوى الإرهابي." متاح عبر: https://gnet-research.org/wp-content/uploads/2020/09/GNET-Report-Decoding-Hate-Using-Experimental-Text-Analysis-to-Classify-Terrorist-Content_ARABIC.pdf

136 انظر: https://www.christchurchcall.com/

137 انظر: https://www.gifct.org/joint-tech-innovation/

138 European Commission, Migration and Home Affairs, Counter-terrorism and radicalisation. https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism_en

139 European Commission, Press Office, EU Internet Forum: Bringing together governments, Europol and technology companies to counter terrorist content and hate speech online. 3 ديسمبر 2015. https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6243

140 European Commission, 'Proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online', COM(2018) 640. 2018/0331. 12 سبتمبر 2018. ص 1 https://eur-lex.europa.eu/resource.html?uri=cellar:dc0b5b0f-b65f-11e8-99ee-01aa75ed71a1.0001.02/DOC_1&format=PDF

وأطلق يوروبول عدة عمليات كبيرة لإزالة تنظيم داعش والمستخدمين المنتسبين إليه عن تليغرام. وعلى مدار عدة أيام من نوفمبر 2019، بلغ عدد الحسابات والبوتات التي أزالها يوروبول 5,055 حسابًا وبوتًا، مقارنة بمتوسط يومي يتراوح من 200 إلى 300 عملية إزالة للحسابات في فترات أخرى.[141] وفي ديسمبر 2018، تمت إزالة 3,276 حسابًا في يوم واحد، وفقًا لتليغرام، وأزالت يوروبول مثل ذلك في يوم آخر من شهر أبريل في وقت سابق من العام نفسه.[142] وفيما تُقوِّض هذه الإجراءات الفردية عملياتِ تنظيم داعش إلى حد كبير، فمن غير المرجح أن يكون لها تأثير دائم ما لم يتحقق الاتساق في جهود القضاء عليها.

وبالتوازي مع أيام القضاء عليها هذه، أدى التعاون بين تليغرام ويوروبول أيضًا إلى تعزيز أدوات إحالة المحتوى التي تُمكِّن أي مستخدم من إحالة المحتوى الذي يعتبره غير مناسب مستعينًا بميزة الإحالة في المجموعات والقنوات.[143]

فرنسا

دعت فرنسا، مع ألمانيا، المفوضية الأوروبية إلى إخضاع تطبيقات المراسلة المشفرة للقواعد التنظيمية كوسيلة للمساعدة في مكافحة الإرهاب.[144] وعندما كان ماتياس فيكل وزيرًا للداخلية الفرنسية، طالب، على وجه التحديد، بأن تتمتع الشرطة بنفس إمكانية الوصول إلى مشغلي الإنترنت والتكنولوجيا مثلما يمكنهم مطالبة شركات الاتصالات بأي معلومات.[145]

ونتيجة للضغوط التي تمارسها فرنسا وألمانيا، تقترح المفوضية الأوروبية تعديل لائحة الخصوصية الإلكترونية في الاتحاد الأوروبي، بما يسمح فعليًا للحكومة الوطنية بتجنب إجراءات حماية الخصوصية المعينة في حالة تعرض الأمن القومي للتهديد – ولكن هذا لا يشمل خضوع التشفير للقواعد التنظيمية.[146] والتحدي الذي يواجه وكالات إنفاذ القانون الوطنية الآن هو افتقارها إلى الأدوات القانونية اللازمة لإجبار شركات التكنولوجيا على إتاحة البيانات المشفرة.[147] ولكن، توقفت المفاوضات على مستوى المجلس وظلت كذلك في ظل الرئاسة الألمانية للاتحاد الأوروبي، منذ نشر مقترحات المفوضية الأوروبية في يناير 2017.[148]

في فرنسا، يُطلب من مقدمي التشفير حاليًا "الدخول في اتفاقيات مع الحكومة لتسهيل إمكانية الوصول إلى البيانات التي يقومون بتشفيرها أو يتعرضون للغرامات".[149] وبالتوازي مع ذلك، يتمتع مكتب رئيس الوزراء بسلطة "حظر خدمات التشفير التي لا تفي بالتزاماتها القانونية".[150]

141 BBC Monitoring, 'Europol disrupts Islamic State propaganda machine', BBC News. 25 نوفمبر 2019. https://www.bbc.com/news/world-middle-east-50545816

142 المرجع نفسه.

143 Europol, Europol and Telegram take on terrorist propaganda online. Press release. 25 نوفمبر 2019. https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online

144 Government of France, Ministry of the Interior, 'Initiative franco allemande sur la securite interieure en Europe'. 23 أغسطس 2016. https://www.interieur.gouv.fr/Archives/Archives-des-actualites/2016-Actualites/Initiative-franco-allemande-sur-la-securite-interieure-en-Europe

145 Stupp, C. 'EU to propose new rules targeting encrypted apps in June', Euractiv. 29 مارس 2017. https://www.euractiv.com/section/data-protection/news/eu-to-propose-new-rules-on-police-access-to-encrypted-data-in-june/

146 المرجع نفسه.

147 المرجع نفسه.

148 European Parliament, Legislative train schedule: Proposal for a regulation on privacy and electronic communications. https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform

149 Lewis, J. A., Zheng, D. E., Carter, W. A. 'The effect of encryption on lawful access to communications and data', CSIS technology policy program. فبراير 2017. ص 20. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf

150 المرجع نفسه.

غانا

نظرًا لأن تجارب غانا في الهجمات الإرهابية محدودة جدًا – لم تقع بها إلا 21 حادثة ولم تخلّف سوى 23 حالة وفاة منذ عام 1970[151] – لم تضع الحكومة الغانية إطارًا قويًا لحوكمة التطرف العنيف عبر الإنترنت.[152]

وعلى عكس غانا، تواجه نيجيريا المجاورة لها في غرب إفريقيا هجمات إرهابية كبيرة منذ سنوات. وشنت بعض الجماعات مثل بوكو حرام وولاية غرب إفريقيا التابعة للدولة الإسلامية هجمات مشينة مثل اختطاف طالبات في أبريل 2014[153] ومذابح يناير 2015، وكلاهما في ولاية بورنو.[154] وبدأت بوكو حرام استخدام منصات التواصل الاجتماعي في إنتاج الدعاية وتجنيد أعضاء جدد لنصرتها. وكثيرًا ما تستخدم هذه الجماعة منصات التواصل الاجتماعي التقليدية، مثل تويتر وفيسبوك ويوتيوب، لنشر صور الجنود، وترويج قطع الرؤوس والخطف، ونشر الرسائل المناهضة للحكومة سعيًا لتجنيد آخرين.[155] ولكن بدأت بوكو حرام في السنوات الأخيرة استخدام تطبيقات المراسلة الفورية المشفرة مثل تليغرام لإصدار مواد دعائية والتنديد بغيرها من الجماعات.[156] وكثفت الحكومة النيجيرية في عام 2013 قوانين مكافحة الإرهاب والحوكمة استجابة لتزايد الإرهاب في البلاد. وعززت مؤسسات الدولة لمكافحة الإرهاب، وتستطيع الحكومة الآن احتجاز ومحاكمة المشتبه فيهم الإرهاب وإصدار عقوبة الإعدام لمن ثبت أنهم ارتكبوا أو يخططون لارتكاب عمل إرهابي.[157]

وفيما يتعلق بإخضاع تليغرام وبدائله للقواعد التنظيمية، اختارت جارة غانا الإقليمية أسلوب حوكمة تقليدي يرتكز على الدولة ومن أعلى إلى أسفل. ويتمحور هذا الشكل من أشكال الحوكمة حول الإجراءات التشريعية، مع قليل من التركيز على المبادرات عبر القطاعات أو مشاركة المجتمع المدني. وثبت أن الحوكمة المرتكزة على الدولة تؤدي إلى نتائج خطيرة غير مرغوبة، منها على سبيل المثال إغلاق الحكومة للإنترنت أو الاستخدام الحكومي لوسائل التواصل الاجتماعي لقمع المعارضة السياسية.[158] وتستعين الحكومات في أفريقيا بإرث من القوانين الاستعمارية العنيفة التي انتُهكت بها حريات المواطنين في الماضي، بهدف "إضفاء الشرعية على العديد من ... محاولات تقديم مطالب غير قانونية للقطاع الخاص."[159] وتضطر منصات وسائل التواصل الاجتماعي ومزودو خدمات الإنترنت أن يستجيبوا لمطالب إغلاق حكومية غير قانونية، ما يثير مخاوف من فرض الرقابة وانتهاك حرية التعبير.[160]

وأعربت جماعات المجتمع المدني والصحفيون عن قلقهم بشأن مستقبل غانا فيما يتعلق بإخضاع الإنترنت ومنصات التواصل الاجتماعي لقواعد تنظيمية.[161] وعلى سبيل المثال، أعلن قائد الشرطة الغانية، قبل الانتخابات الوطنية عام 2016، عن احتمال إغلاق وسائل التواصل الاجتماعي (ولم يحدث لحسن الحظ).[162] وتترك قوانين حرية

151 قاعدة بيانات الإرهاب العالمي، START. متاح عبر: https://www.start.umd.edu/gtd/

152 انظر أيضًا: قسم المشهد السياسي في تقرير GNET السابق، "الذكاء الاصطناعي ومكافحة التطرف العنيف: كتاب تمهيدي". متاح عبر: https://gnet-research.org/wp-content/uploads/2020/09/GNET-Report-Artificial-Intelligence-and-Countering-Violent-Extremism-A-Primer_ARABIC.pdf

153 Mbah, F. (2019), 'Nigeria's Chibok schoolgirls: Five years on, 112 still missing,' Al Jazeera. متاح عبر: https://www.aljazeera.com/news/2019/4/14/nigerias-chibok-schoolgirls-five-years-on-112-still-missing

154 Amnesty International (2018), 'Boko Haram Baga attacks: satellite images reveal destruction.' متاح عبر: https://www.amnesty.org.uk/nigeria-boko-haram-doron-baga-attacks-satellite-images-massacre

155 UN Development Programme and RAND (2018), 'Social Media in Africa.' متاح عبر: https://www.africa.undp.org/content/rba/en/home/library/reports/social-media-in-africa-.html

156 Zenn, J. (2017), 'Electronic Jihad in Nigeria: How Boko Haram is Using Social Media,' Terrorism Monitor, vol. 15, no. 23. متاح عبر: https://www.refworld.org/docid/5b728ca2a.html

157 'Nigeria: Extremism & Counter Extremism,' Counter-Extremism Project. متاح عبر: https://www.counterextremism.com/countries/nigeria

158 Ilori, T. (2020), 'Content Moderation Is Particularly Hard in African Countries,' Information Society Project at Yale Law School. متاح: https://law.yale.edu/isp/initiatives/wikimedia-initiative-intermediaries-and-information/wiii-blog/moderate-globally-impact-locally-content-moderation-particularly-hard-african-countries

159 Ilori, T. (2020), 'Stemming digital colonialism through reform of cybercrime laws in Africa,' Information Society Project at Yale Law School. متاح: https://law.yale.edu/isp/initiatives/wikimedia-initiative-intermediaries-and-information/wiii-blog/stemming-digital-colonialism-through-reform-cybercrime-laws-africa

160 'Ranking Digital Rights, '2019 RDR Corporate Accountability Index'. متاح: https://rankingdigitalrights.org/index2019/assets/static/download/RDRindex2019report.pdf

161 Majama, K. (2019) 'Africa in urgent need of a homegrown online rights strategy,' Association for Progressive Communications. متاح: https://www.apc.org/en/news/africa-urgent-need-homegrown-online-rights-strategy

162 Olukotun, D. 'President of Ghana says no to internet shutdowns during coming elections,' AccessNow، 16 أغسطس 2019. متاح: https://www.accessnow.org/president-ghana-says-no-internet-shutdown-elections-social-media/

التعبير السخية في غانا الفضاء الرقمي عرضةً للانتهاكات، مثل خطاب الكراهية والتنمر السيبراني (على النساء خصوصًا).[163] لذا تتزايد الدعوات لإحكام القواعد التنظيمية على منصات وسائل التواصل الاجتماعي.

وتلبيةً لهذه الدعوات، أقرت غانا مشروع قانون الحق في المعلومات في عام 2019، والذي يضمن إمكانية الوصول إلى المعلومات التي تحتفظ بها المؤسسات العامة.[164] ويشير مشروع القانون إلى أن الحكومة الغانية تريد التعامل مع الحقوق الرقمية بشفافية ومساءلة، وتحقيق التوازن بين حماية المستخدمين من الضرر وصون حريتهم في التعبير. ومع ذلك، تستطيع الحكومة الغانية أن تتوسع في استراتيجيتها لمكافحة التطرف العنيف على نحو يعزز تعاونها مع المجتمع المدني والمجموعات المجتمعية ومشاركتهم في الاستجابة للتحديات.

اليابان

تفرق جهود الحكومة اليابانية لمكافحة الإرهاب بوضوح تام بين ما تعتبره أنشطة إرهابية أجنبية ومحلية. وهكذا تنقسم مسؤلية المؤسسات إلى نهجيْن مختلفيْن في مواجهة التطرف العنيف على الإنترنت.

وفيما يتعلق بالتهديدات المحلية، كتلك التي تشكلها دورة الألعاب الأولمبية طوكيو 2021 أو اليمين المتطرف الياباني، تقوم جهات إنفاذ القانون بتنسيق استجابة الدولة لها إلى حد كبير. ولا تزال أنشطة التخريب الشيوعية التي تعود إلى حقبة الحرب الباردة تؤثر على طريقة تعامل اليابان مع التهديدات المحلية: تتولى شرطة المحافظات (التي تشرف عليها وكالة الشرطة الوطنية) ووكالة استخبارات الأمن العام (وكالة الاستخبارات الوطنية اليابانية) جمع المعلومات الاستخبارية وجهود مكافحة الإرهاب في اليابان.[165]

وبالتالي، تتمحور أنشطة مكافحة الإرهاب المحلية حول هياكل الشرطة والأمن التقليدية. وحيث أن اليابان تميل إلى التطورات التكنولوجية المبتكرة، فقد قطعت شوطًا في إيجاد حلول يقودها الذكاء الاصطناعي، بما فيها التعرف على الوجوه على نطاق واسع، والتحقق البيومتري وأنظمة الكشف عن السلوك.[166] وتقترح هذه الحلول نموذجًا للحوكمة يتمحور حول الاكتشاف المبكر والوقاية، ويتم تفعيلها من خلال تكتيكات الشرطة والأمن التقليدية.

ولتعزيز هذه الجهود، روَّج رئيس الوزراء الياباني شينزو آبي مشروع قانون[167] لمكافحة الإرهاب في منتصف عام 2017 وصفه زعيم المعارضة الياباني بأنه "وحشي".[168] ويجرم هذا التشريع التخطيط لارتكاب أكثر من 270 "جريمة خطيرة"، ومنها الاعتصام وانتهاكات حقوق النشر الموسيقية، ويمتد تطبيقه ليشمل وسائل التواصل

163 Endert, J. (2018) 'Digital backlash threatens media freedom in Ghana,' DW Akademie. متاح: https://www.dw.com/en/digital-backlash-threatens-media-freedom-in-ghana/a-46602904

164 Yahya Jafru, M. 'Right to information – RTI bill passed into law,' Graphic Online، 26 مارس 2019. متاح: https://www.graphic.com.gh/news/politics/ghana-news-rti-bill-passed.html

165 Kotani, K., 'A Reconstruction of Japanese Intelligence: Issues and Prospects', in Philip H. J. Davies & Kristian C. Gustafson (eds.), Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere (Washington D.C.: Georgetown University Press, 2013), pp. 181–99.

166 The Government of Japan, 'All is Ready for a Safe and Secure Tokyo Games'، خريف/شتاء 2019. متاح: https://www.japan.go.jp/tomodachi/2019/autumn-winter2019/tokyo2020.html؛
'NEC Becomes a Gold Partner for the Tokyo 2020 Olympic and Paralympic Games,' NEC Corporation, 2015'. متاح: https://www.nec.com/en/press/201502/global_20150219_01.html؛
Kyodo News, 'Kanagawa police eye AI-assisted predictive policing before Olympics'، 29 يناير 2018. متاح عبر: https://english.kyodonews.net/news/2018/01/5890d824baaf-kanagawa-police-eye-ai-assisted-predictive-policing-before-olympics.html

167 The Bill passed via "the unusual step of skipping a vote in the Upper House Committee on Judicial Affairs." Japan Federation of Bar Associations, 'Statement on the Enactment of the Bill to Revise the Act on Punishment of Organized Crimes and Control of Crime Proceeds, including the Criminalization of Conspiracy'، 15 يونيو 2017. متاح عبر: https://www.nichibenren.or.jp/en/document/statements/170615.html

168 Allen-Ebrahimian, B., 'Japan Just Passed a "Brutal," "Defective" Anti-Terror Law', Foreign Affairs، 16 يونيو 2017. متاح عبر: https://foreignpolicy.com/2017/06/16/japan-just-passed-a-brutal-defective-anti-terror-law/

الاجتماعي.[169] ويشعر نشطاء الحقوق المدنية وجماعات المجتمع المدني بقلق بالغ من مشروع القانون، بسبب الصلاحيات والسلطات الواسعة التي يمنحها لمراقبة وتتبع النشاط على الإنترنت.[170]

وفيما يتعلق بالجهود الدولية لمكافحة الإرهاب، يخفف نهج اليابان تركيزه المحلي على التجريم. وتبذل اليابان جهودًا لمكافحة الإرهاب في الخارج وجهودًا إقليمية وجهودًا لبناء القدرات وتعزيز التعاون. وكثيرٌ من جهودها لمكافحة التطرف العنيف تقع، على وجه التحديد، ضمن رابطة دول جنوب شرق آسيا (آسيان)،[171] التي أصدرت مجموعة من البيانات التوضيحية التي تلزم الموقعين عليها "بمنع الإرهاب الدولي وتعطيله ومكافحته بتبادل المعلومات وتبادل الاستخبارات وبناء القدرات"، ما يُعد سابقة في التعاون الإقليمي لمكافحة التطرف العنيف والإرهاب.[172]

واستضافت اليابان مرتين الحوار السنوي لمكافحة الإرهاب بين الآسيان واليابان، فضلاً عن مشاركتها في محادثات ثنائية مع مجموعة من الجهات الفاعلة العالمية.[173] وفي أواخر عام 2019، أجرت اليابان والمملكة المتحدة مناقشات حول "الوضع الحالي للإرهاب الدولي، والتدابير المحلية لمكافحة الإرهاب، وكذلك بشأن التعاون الحالي في بناء القدرات لمكافحة الإرهاب، ولا سيما في البلدان الأخرى[sp.]."[174]

ومن المرجح أن تلتزم بهذا النهج المشترك في مكافحة استخدام المتطرفين لتليغرام وبدائله في اليابان: استراتيجية مواجهة خارجية للتعاون الإقليمي ووضع جدول الأعمال، مع تفعيلها محليًا على أساس الأنشطة الأمنية والشرطية وأنشطة المراقبة التقليدية.

نيوزيلندا

صدرت استراتيجية نيوزيلندا الشاملة لمكافحة الإرهاب في فبراير 2020، وتوضح أن حوكمة مكافحة التطرف العنيف عبر الإنترنت تتضمن التنسيق بين مختلف الوكالات والهيئات.[175] ومثلما حدث في كندا (أعلاه)، تضم هذه الهيئات لجنة العلاقات الخارجية والأمن التابعة لمجلس الوزراء وأجهزة الشرطة والاستخبارات والاتصالات الأمنية ووكالات الشؤون الخارجية والتجارة والدفاع والنقل والابتكار والتنمية.

وحظيت نيوزيلندا باهتمام دولي لدورها القيادي في المبادرات عبر البلدان والقطاعات. والجدير بالذكر أن حكومتيْ نيوزيلندا وفرنسا كوَّنتا، في أعقاب إطلاق النار على المصلين في مسجد كرايستشيرش في مارس 2019، تحالفًا من رؤساء الدول مع شركات وسائل التواصل الاجتماعي والتكنولوجيا في إطار دعوة كرايستشيرش للقضاء على المحتوى الإرهابي والعنف والمحتوى المتطرف عبر الإنترنت.[176] وتلزم الدعوة الموقعين عليها بإنفاذ القوانين التي تحظر نشر المحتوى الإرهابي والمتطرف العنيف عبر الإنترنت، واحترام حرية التعبير والخصوصية. وتعمل هذه البلدان أيضًا على دعم الأطر وأنشطة بناء القدرات وتعزيز الوعي لمنع استغلال الخدمات عبر الإنترنت لنشر المحتوى الإرهابي والمتطرف العنيف.

---

169 McCurry, J., 'Japan passes "brutal" counter-terror law despite fears over civil liberties', The Guardian، 15 يونيو 2017. متاح عبر: https://www.theguardian.com/world/2017/jun/15/japan-passes-brutal-new-terror-law-which-opponents-fear-will-quash-freedoms; Adelstein, J., 'Japan's Terrible Anti-Terror Law Just Made "The Minority Report" Reality,' The Daily Beast، 15 يونيو 2017. متاح عبر: http://www.thedailybeast.com/japans-terrible-anti-terror-law-just-made-the-minority-report-reality

170 Japan Federation of Bar Associations, 'Statement on the Enactment of the Bill to Revise the Act on Punishment of Organized Crimes and Control of Crime Proceeds, including the Criminalization of Conspiracy'، 15 يونيو 2017. متاح عبر: https://www.nichibenren.or.jp/en/document/statements/170615.html

171 'Japan: Extremism & Counter Extremism,' Counter-Extremism Project. متاح: https://www.counterextremism.com/countries/japan

172 'ASEAN-Japan Joint Declaration for Cooperation to Combat International Terrorism' ASEAN. متاح: https://asean.org/?static_post=asean-japan-joint-declaration-for-cooperation-to-combat-international-terrorism-2

173 'Japan: Extremism & Counter Extremism,' Counter-Extremism Project. متاح: https://www.counterextremism.com/countries/japan

174 'The 4th Japan-the UK Counter-Terrorism Dialogue' Ministry of Foreign Affairs of Japan، 4 ديسمبر 2019. متاح عبر: https://www.mofa.go.jp/fp/is_sc/page1e_000297.html

175 Government of New Zealand, Officials' Committee for Domestic and External Security Coordination, 'Countering terrorism and violent extremism national strategy overview' Counter-Terrorism Coordination Committee، فبراير 2020. https://dpmc.govt.nz/sites/default/files/2020-02/2019-20 CT Strategy-all-final.pdf

176 انظر: https://www.christchurchcall.com/

كما تلزم دعوة كرايستشيرش الشركات، ومنها أمازون وفيسبوك وغوغل وتويتر ويوتيوب، بمعايير الصناعة الأكبر التي تعزز المساءلة والشفافية. ويجب على الشركات فرض معايير المجتمع وشروط الخدمات بإيلاء الأولوية لعمليات إدارة المحتوى وإزالته، والتعرف على المحتوى لحظة بلحظة لمراجعته وتقييمه. وتعمل البلدان والشركات معًا على تطوير جهودها مع المجتمع المدني لتعزيز أنشطة المجتمع المدني للتدخل في عمليات الراديكالية عبر الإنترنت.

وكانت هذه الدعوة أيضًا بمثابة وسيلة الإصلاح الشامل لمنتدى الإنترنت العالمي لمكافحة الإرهاب (GIFCT). وفي إطار عملية الإصلاح الشامل هذه، تعددت صلاحيات منتدى الإنترنت العالمي لمكافحة الإرهاب (GIFCT) وشملت مجموعة من الأنشطة الوقائية وتدابير الاستجابة والأنشطة التعليمية اللازمة لمكافحة التطرف العنيف عبر الإنترنت.[177]

تطرح جهود نيوزيلندا للمشاركة في رعاية مجموعة من المبادرات العالمية عبر القطاعات نهجًا أفقيًا أكثر لحوكمة استخدام المتطرفين لمنصات التكنولوجيا. ويشمل هذا النهج هياكل الأمن والاستخبارات التقليدية بالإضافة إلى المبادرات التي تجمع الممارسين والأوساط الأكاديمية وصناع السياسات وقادة التكنولوجيا لصياغة استجابات مناسبة للتهديدات المتطرفة العنيفة الناشئة عبر الإنترنت.

المملكة المتحدة

يتبع نهج المملكة المتحدة في مكافحة الاستخدام المتطرف للمنصات عبر الإنترنت نمطًا تقليديًا للحوكمة يركز على مؤسسات الدولة. ووزارة الداخلية هي المؤسسة المركزية المسؤولة عن تشريعات مكافحة الإرهاب، وذلك بالتنسيق أيضًا مع مقر الاتصالات الحكومية (Government Communications Headquarters)، والمؤسسات الأمنية والاستخباراتية في البلاد. وأنشأت وزارة الداخلية أيضًا هيئات تعاونية مع مؤسسات حكومية أخرى (غالبًا وزارة الرقمية والثقافة والإعلام والرياضة) والبرلمان، مثل مجلس المملكة المتحدة للأمان على الإنترنت والمكتب الوطني الأمني لمكافحة الإرهاب ومفوضية مكافحة التطرف.[178]

تتبع المملكة المتحدة، على غرار اليابان (أعلاه)، نهجًا ذا شقين لمواجهة التطرف العنيف عبر الإنترنت. ويتمحور مسار نشاطها الأول حول إخضاع وسائل التواصل الاجتماعي ومنصات التكنولوجيا لقواعد تنظيمية. حدد كتاب الحكومة الأبيض بشأن الأضرار على الإنترنت (Online Harms White Paper)، الذي نُشر في أبريل 2019، حالة نموذجية شاملة لمزيد من التنظيم الوطني لوسائل التواصل الاجتماعي.[179] وحسب هذا الإطار التنظيمي الجديد، سوف تتحمل وسائل التواصل الاجتماعي وشركات التكنولوجيا واجبًا قانونيًا جديدًا يتمثل في رعاية مستخدميها، وتتولى Ofcom تنفيذه بصفتها الهيئة التنظيمية للاتصالات في المملكة المتحدة. وسوف تفرض هيئة Ofcom على المنصات عقوبات مالية وتقنية – يمكن حظر مواقع الويب على مستوى مزود خدمة الإنترنت وفرض غرامة تصل إلى 4٪ من إيراداتها العالمية – عند عدم الامتثال لإطار العمل وانتهاك واجب الرعاية القانوني.[180] وفي وقت كتابة هذا التقرير، تأخر مشروع قانون الأضرار على الإنترنت، التنفيذ التشريعي للكتاب الأبيض، لعدة سنوات.[181]

177 Global Internet Forum to Counter Terrorism, 'Next Steps for GIFCT'، 23 سبتمبر 2019. متاح عبر: https://gifct.org/press/next-steps-gifct/

178 Gov.uk, UK Council for Internet Safety. متاح عبر: https://www.gov.uk/government/organisations/uk-council-for-internet-safety؛
Gov.uk, Commission for Countering Extremism. متاح عبر: https://www.gov.uk/government/organisations/commission-for-countering-extremism؛
Gov.uk, National Counter Terrorism Security Office. متاح عبر: https://www.gov.uk/government/organisations/national-counter-terrorism-security-office

179 HM Government, 'Online Harms White Paper'، أبريل 2019. متاح: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

180 Crawford, A. 'Online Harms bill: Warning over "unacceptable" delay,' BBC، 29 يونيو 2020. متاح: https://www.bbc.co.uk/news/technology-53222665

181 المرجع نفسه.

ويركز النهج الثاني الذي تتبعه المملكة المتحدة على مؤسسات الشرطة التقليدية والمؤسسات الأمنية والاستخباراتية، مدعومًا بتشريعات مكافحة الإرهاب ومساندة شعبية قوية. وفي ربيع 2020، قدم البرلمان تشريعات مقترحة جديدة لمكافحة الإرهاب تستهدف المشتبه في ارتكابهم أنشطة إرهابية. وحسب هذه التشريعات الجديدة، فإن المشتبه به "الذي لم يدان بأي جريمة قد يخضع لإجراءات مراقبة موسعة ومتزايدة."[182] ولن تخضع تدابير المراقبة هذه بعد الآن للحد الزمني المعروف وهو عامان. فضلاً عن أن تدابير منع الإرهاب والتحقيق فيه (المعروفة باسم Tpims)، ومنها النقل الإلزامي، ووضع علامات المراقبة الإلكترونية، والإقصاء عن أماكن محددة، والقيود المفروضة على السفر، والجمعيات، والخدمات المالية، واستخدام الاتصالات، سيكون من الأسهل فرضها الآن في إطار التخفيف من عبء تقديم البينة المقترح.[183]

وجاءت هذه التدابير الصارمة لمكافحة الإرهاب في أعقاب الهجمات التي تعرضت لها قاعة فيشمونغرز في مدينة لندن في نوفمبر 2019 وعلى طريق ستريتام السريع في فبراير 2020،[184] على خلفية دعم الرأي العام وضع تشريعات صارمة.[185] ونظرًا لهذه الروح المتساهلة، فإن مناهج مكافحة التطرف العنيف عبر الإنترنت، لاسيما استخدام تطبيقات مثل تليغرام وبدائله، قد تحيد عن النهج التنظيمي نحو نهج يعزز تطبيق القانون. وبموجب مشروع القانون المقترح، سوف يُخفف عبء البينة لإخضاع مواطن لتدابير منع الإرهاب والتحقيق (Tpims) إلى "أسباب معقولة".[186] ولم يتضح بعد إذا كان استخدام تطبيقات مثل تليغرام وتطبيقات المراسلة الفورية النصية الأخرى اللامركزية والمشفرة للوصول إلى المحتوى المتطرف أو نشره سوف يُعتبر من بين هذه الأسباب المعقولة.

المديرية التنفيذية للجنة الأمم المتحدة لمكافحة الإرهاب

اعتمدت الجمعية العامة للأمم المتحدة بالإجماع استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب في عام 2006. ومنذ ذلك الحين، اتخذ مجلس الأمن قرارات تركز على التصدي للإرهاب وتتطلب من الدول الأعضاء التعاون الكامل في مكافحة الإرهاب. ويتطلب القراران 1373 (2001) و 1566 (2004) "اتخاذ إجراءات تشريعية من قبل جميع الدول الأعضاء لمكافحة الإرهاب، بما في ذلك زيادة التعاون مع الحكومات الأخرى."[187] ويعترف القرار 1963 (2010) بتزايد استخدام الإنترنت من قبل الإرهابيين لأغراض إرهابية.[188]

وتطرح معالجة استخدام المنظمات الإرهابية للمنصات اللامركزية تحديات أمام وكالات إنفاذ القانون. ولا تحتاج هذه المنصات وسيطًا لإرسال الرسائل واستقبالها، ما يجعل تعقب الإرهابيين (المشتبه بهم) أمرًا صعبًا للغاية.[189]

ودعت الأمم المتحدة حكومات الدول إلى توفير "أساس قانوني واضح للالتزامات الواقعة على أطراف القطاع الخاص" والتي بموجبها ينبغي أن تتعاون شركات ومنصات التكنولوجيا مع سلطات إنفاذ القانون أثناء التحقيقات.[190]

---

182 'United Kingdom: Extremism & Counter Extremism,' Counter-Extremism Project. متاح عبر: https://www.counterextremism.com/countries/unitedkingdom

183 Grierson, J., 'Unconvicted terrorism suspects face indefinite controls under UK bill,' The Guardian، 20 مايو 2020. متاح عبر: https://www.theguardian.com/politics/2020/may/20/unconvicted-terrorism-suspects-face-indefinite-controls-under-uk-bill

184 'Department of Justice, 'Press release: 14-year minimum jail terms for most dangerous terror offenders'، 20 مايو 2020. متاح عبر: https://www.gov.uk/government/news/14-year-minimum-jail-terms-for-most-dangerous-terror-offenders

185 حسب تقرير صدر في سبتمبر 2017 وتضمن استطلاعًا للمواقف المتخذة تجاه المحتوى المتطرف عبر الإنترنت، يؤيد نحو ثلاثة أرباع المشاركين في الاستطلاع صدور تشريع جديد يجرم امتلاك واستغلال المحتوى المتطرف عبر الإنترنت. انظر: Frampton, M. (2017), 'The New Netwar: Countering Extremism Online,' Policy Exchange. متاح عبر: https://policyexchange.org.uk/wp-content/uploads/2017/09/The-New-Netwar-1.pdf

186 Amnesty International UK, 'Counter-Terrorism and Sentencing Bill 2019-21: Submission to the Public Bill Committee'، يونيو 2020. متاح عبر: https://publications.parliament.uk/pa/cm5801/cmpublic/CounterTerrorism/memo/CTSB07.pdf

187 UNODC, The use of the Internet for terrorist purposes. الأمم المتحدة، 2012. ص 16 https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

188 المرجع نفسه.

189 Tech Against Terrorism, Analysis: ISIS use of smaller platforms and the DWeb to share terrorist content. أبريل 2019. https://www.voxpol.eu/isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content/

190 UNODC, 2012. p. 135

الولايات المتحدة

يمكن وصف نهج سياسة الولايات المتحدة لمكافحة إساءة استخدام منصات التكنولوجيا بأنه غير منتظم. وفيما يتعلق بمؤسسات الدولة المعنية، فإن وزارة الأمن الداخلي (DHS)، ووزارة العدل، ومكتب التحقيقات الفيدرالي، والمركز الوطني لمكافحة الإرهاب، ومجلس الأمن القومي والكونغرس، وغيرهم، في طليعة جهود الاستجابة.[191] وجُربت مجموعة من الأساليب: "الرسائل المضادة، وجلسات التوعية، والشراكات، والتشريعات."[192]

ومن هذه الأساليب المشاركة في رعاية المبادرات العالمية المشتركة بين القطاعات. وتُلزم إستراتيجية الولايات المتحدة لمكافحة الإرهاب نفسها بالعمل مع قطاع الأعمال والصناعة لمكافحة تجنيد الإرهابيين وجمع الأموال والراديكالية عبر الإنترنت. وفيما يتعلق بالمبادرات عبر الوطنية، تعمل الولايات المتحدة الأمريكية مع مبادرات مثل Tech Against Terrorism (التكنولوجيا في مواجهة الإرهاب) والمنتدى العالمي لمكافحة الإرهاب، والتي تعتمد على الشراكة مع الموقعين الآخرين والمجتمع المدني وقطاع التكنولوجيا لصياغة نُهج متوسطة المدى وبعيدة المدى لمكافحة التطرف العنيف عبر الإنترنت.

وعلى نطاق أوسع، أطلقت إدارة أوباما فرقة عمل لمكافحة التطرف العنيف في عام 2011، من أجل "توحيد الجهود المحلية لمكافحة التطرف العنيف."[193] وتهدف فرقة العمل إلى الجمع بين الممارسين من الهيئات المذكورة أعلاه لتنسيق المشاركة مع المجتمع المدني، وتطوير نماذج التدخل، والاستثمار في البحوث والنهوض بالاتصالات والاستراتيجيات الرقمية.[194] وبالنظر إلى الجهود المتفرقة السابقة التي بذلتها الولايات المتحدة الأمريكية، فإن اتباع نهج موحد لمواجهة التطرف العنيف عبر الإنترنت قد يعزز الجهود المبذولة لمكافحة إساءة استخدام المنصات مثل تليغرام.

ولكن، في أوائل عام 2017، نظر الرئيس ترامب في إعادة هيكلة فرقة العمل لإزالة إرهاب التفوق الأبيض من نطاق اختصاصه، وإعادة تسمية هذا البرنامج باسم "مكافحة التطرف الإسلامي الراديكالي."[195] وعلاوة على ذلك، قُطعت جميع التمويلات المخصصة لبرامج مكافحة التطرف العنيف من الميزانية التي تم الكشف عنها في ربيع 2017.[196] وبحلول أواخر أكتوبر 2018، توقف نشاط فرقة العمل: انتهى التمويل و "عاد الموظفون إلى وكالاتهم وإداراتهم الأصلية."[197]

وتكشف تصرفات ترامب عن عداء عميق لجهود مكافحة التطرف العنيف عمومًا، ولاسيما التي تهدف إلى التواصل المجتمعي والمشاركة مع المجتمع المدني المحلي والتي تستهدف اليمين المتطرف والإرهاب العنصري الأبيض. وعلى سبيل المثال، حصلت مبادرة "الحياة بعد الكراهية" على تمويل من وزارة الأمن الداخلي (DHS)، وهي مبادرة تعمل مع الأفراد لمساعدتهم على الانشقاق عن مجموعات البيض العنصرية والنازيين الجدد.[198] ويمكن فهم قطع التمويل وتقليص الصلاحيات لاستبعاد التفوق الأبيض من جهود الولايات المتحدة الأمريكية كإشارة صارخة إلى أن إدارة ترامب لن تتخذ إجراءات ضد البيض العنصريين ولا الأعمال الإرهابية العنصرية.

---

191 Alexander, A. (2019), 'A Plan for Preventing and Countering Terrorist and Violent Extremist Exploitation of Information and Communications Technology in America,' George Washington University Program on Extremism، ص 5. متاح عبر: https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/A%20Plan%20for%20Preventing%20and%20Countering%20Terrorist%20and%20Violent%20Extremist.pdf

192 المرجع نفسه.

193 Department of Homeland Security, 'Countering Violent Extremism Task Force'. متاح عبر: https://www.dhs.gov/cve/task-force

194 المرجع نفسه.

195 Ainsley, J. et al., 'Exclusive: Trump to focus counter-extremism program solely on Islam – sources,' Reuters، 3 فبراير 2017. متاح عبر: https://www.reuters.com/article/idUSKBN15G5VO?feedType=RSS&feedName=topNews&utm_source=twitter&utm_medium=Social

196 Ainsley, J., 'White House budget slashes 'countering violent extremism' grants,' Reuters، 23 مايو 2017. متاح عبر: https://www.reuters.com/article/us-usa-budget-extremism-idUSKBN18J2HJ

197 Beinart, P. 'Trump Shut Programs to Counter Violent Extremism,' The Atlantic، 29 أكتوبر 2018. متاح عبر: https://www.theatlantic.com/ideas/archive/2018/10/trump-shut-countering-violent-extremism-program/574237/

198 Life After Hate, 'About Us'. متاح عبر: https://www.lifeafterhate.org/about-us-page

ولهذا التطور أهمية كبيرة في مكافحة استخدام تليغرام وتطبيقات المراسلة الفورية الأخرى المشفرة واللامركزية. وكما أوضح بينيت كليفورد أعلاه، تستخدم جماعات اليمين المتطرف العديد من هذه المنصات لتنسيق الأنشطة. وإذا ثبت الآن أن الاستجابات الحكومية لهذه المنصات "ذات دوافع سياسية وخطيرة"،[199] استطعنا أن نلقي نظرة معقولة يشوبها القلق على مستقبل مكافحة التطرف العنيف. ويكمن خط الدفاع الأخير ضد استغلال هذه المنصات في زيادة الضغوط على مؤسسيها للامتثال لأوامر إنفاذ القانون وأوامر المحكمة، وهو نهج سوف يثبت بالتأكيد أنه قليل جدًا ومتأخر جدًا.

نحو طريقة لامركزية لحوكمة المنصات اللامركزية؟

وفي التقرير أعلاه، يحذر بينيت كليفورد من تزايد إقبال التطبيقات الشبيهة بتليغرام على استضافة الخوادم اللامركزية. وظهرت هذه الميزة مع ظهور Web 2.0، وقد تمكّن المستخدمين من التواصل كل منهم مع الآخر مباشرة، ما يعني أنها تتجاوز الخدمات المركزية التي تقدمها شركات مثل غوغل وأمازون وميكروسوفت وفيسبوك.[200] ويتسم النموذج اللامركزي بأنه "يعكس نموذج ملكية البيانات الحالي"، بحيث يُمنح المستخدمون حق ملكية بياناتهم وإمكانية الوصول إليها بالكامل.[201]

وتوفير الخدمة المركزية المملوكة للحكومة يمهد السبيل لسوء المعاملة والمراقبة وفرض الرقابة. على سبيل المثال، فرضت الحكومة الهندية أطول إغلاق للإنترنت في العالم في كشمير في إطار العنف والفظائع التي تُرتكب ضد المسلمين منذ عقود.[202] ودام هذا الإغلاق 192 يومًا، في إطار اتجاه أوسع نطاقًا ومثير للقلق إزاء الحقوق الرقمية في الهند: شكك وزير الاتصالات وتكنولوجيا المعلومات في حق المواطنين في استخدام الإنترنت، مصرحًا بأن "أمن البلاد لا يقل أهمية عن الحق في الإنترنت … هل ننكر [أن] الإرهابيون يسيئون استخدام الإنترنت؟"[203]

وبالمثل، نعلم أن هناك شركات تسيء استخدام بيانات المستخدمين. وفي عام 2018، جمعت مؤسسة الاستشارات السياسية Cambridge Analytica ملايين البيانات الشخصية لمستخدمي فيسبوك لاستخدامها في الدعاية السياسية.[204]وهذا هو أكبر انتهاك للبيانات في تاريخ فيسبوك، واستغله المرشح الرئاسي دونالد ترامب في عام 2016 في استهداف من حددوا أنهم ناخبون متأرجحون من مستخدمي فيسبوك.[205]ولأن بيانات المستخدمين متمركزة على خوادم فيسبوك، تستطيع المنصة التربح من مليارات المعلومات الحساسة والشخصية عنهم ومراقبتها واستغلالها.[206]

وفيما يحتفظ نموذج الإنترنت اللامركزي بالبيانات بعيدًا عن متناول من هب ودب لحمايتها، يفرض أيضًا ثمة تحديات. وخصوصًا أن تطبيقات المراسلة الفورية اللامركزية والمشفرة، بما فيها تليغرام وبدائله، تقدم ملاذًا آمنًا للمحتوى المتطرف. وحسب كليفورد أعلاه، فإن ميزة استضافة الخوادم اللامركزية على المنصات الناشئة

199 Southern Poverty Law Center, 'Trump's planned changes to government's "Countering Violent Extremism" program are politically motivated, dangerous', 2 فبراير 2017. متاح عبر: https://www.splcenter.org/news/2017/02/02/splc-trumps-planned-changes-governments-countering-violent-extremism-program-are

200 Corbyn, Z. 'Decentralisation: The Next Big Step for the World Wide Web,' The Guardian، 8 سبتمبر 2018. متاح عبر: https://www.theguardian.com/technology/2018/sep/08/decentralisation-next-big-step-for-the-world-wide-web-dweb-data-internet-censorship-brewster-kahle

201 Bodó, L. 'Decentralised Terrorism: The Next Big Step for the So-Called Islamic State (IS)?' VoxPol، 12 ديسمبر 2018. متاح عبر: https://www.voxpol.eu/decentralised-terrorism-the-next-big-step-for-the-so-called-islamic-state-is/

202 Pandit, I. 'India is escalating Kashmir conflict by painting it as terrorism,' openDemocracy، 2 ديسمبر 2019. متاح عبر: https://www.opendemocracy.net/en/openindia/india-escalating-kashmir-conflict-painting-it-terrorism/

203 Shastry, V. 'Asia's Internet Shutdowns Threaten the Right to Digital Access,' Chatham House، 18 فبراير 2020. متاح عبر: https://www.chathamhouse.org/2020/02/asias-internet-shutdowns-threaten-right-digital-access

204 Confessore, N. 'Cambridge Analytica and Facebook: The Scandal and the Fallout So Far,' The New York Times، 4 أبريل 2018. متاح عبر: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

205 Hilder, P. and Lewis, P. 'Leaked: Cambridge Analytica's Blueprint for Trump's Victory,' The Guardian، 23 مارس 2018. متاح عبر: https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory

206 Kamyshev, P. 'Facebook's Political Problems are Inherent to Centralized Social Media,' Palladium Magazine، 14 فبراير 2019. متاح عبر: https://palladiummag.com/2019/02/14/facebooks-political-problems-are-inherent-to-centralized-social-media/

"سوف تضع هذه المنصات حتمًا في متناول الجماعات المتطرفة أكثر من غيرها." وتستطيع المنصة اللامركزية الإفلات بسهولة أكبر من المراقبة والتدخل من المنصات ذاتية التنظيم وأوامر إنفاذ القانون، لأن البيانات لم تعد في متناولهم.

وتطرح مكافحة استغلال وإساءة استخدام منصات المراسلة الفورية اللامركزية أسئلةً ملحةً وصعبةً عن الحوكمة. وكيف تستجيب الحكومات والشركات لاستخدام المتطرف للإنترنت اللامركزي؟ وكيف نوازن بين حقوق المستخدمين في الخصوصية وحرية التعبير وبين استغلال المستخدمين المنصات في نشر الدعاية والمعلومات المضللة والتجنيد لنصرة قضاياهم والتخطيط لهجمات إرهابية؟

وهناك ثلاثة سبل محتملة، ضمن أنماط الحوكمة الحالية، يرتبط كل منها على نطاق واسع بمرحلة معينة بطول العملية الخطية للتطرف.

النهج الأول – الوقاية المبكرة – يهدف إلى التدخل في مراحل التطرف الأولى لمنع الناس من الانخراط في المحتوى الإرهابي. أما التطبيقات التي تشبه تليغرام، فقد يصلح نهج الوقاية المبكرة لمنع الناس من السعي إلى التعامل مع المحتوى والجماعات والقنوات المتطرفة على المنصة. وتكمن فائدة هذا النهج في أنه يخفف الرقابة الكثيفة الموارد على المنصة ويضعف وجود المتطرفين عبر الإنترنت مع الحفاظ على حرية المستخدمين في التعبير وحقهم في الخصوصية.

ومع ذلك، فإن برامج الوقاية المبكرة نفسها غارقة في تحديات أخلاقية وسياسية وقانونية أخرى. ولعل أشهر برامج الوقاية المبكرة استراتيجية الوقاية (Prevent Strategy) التي أدخلتها وزارة الداخلية البريطانية في عام 2003. وتستهدف هذه الإستراتيجية "الأفراد المعرضين للتجنيد"، لاسيما داخل المؤسسات مثل مؤسسة NHS والمدارس والجامعات وغيرها من المجتمعات المحلية ومجموعات المجتمع المدني.[207] وتتعرض استراتيجية Prevent منذ إنشائها لانتقادات جماعات الحريات المدنية: ويرى شامي تشاكرابارتي، مدير Liberty آنذاك، وهي مجموعة بارزة معنية بالحقوق المدنية، أن إستراتيجية Prevent "أكبر برنامج تجسس في بريطانيا في العصر الحديث"، لأن المعلومات الاستخبارية التي تُجمع عن من يُسمون بالأفراد المعرضين تتضمن وجهات نظر سياسية ودينية ومعلومات عن صحتهم العقلية ونشاطهم الجنسي.[208] وتستهدف إستراتيجية Prevent المسلمين البريطانيين دون تفرقة بين الغث والسمين، وتدعم الإسلاموفوبيا والخلط بين "المقاومة السياسية المشروعة بين الشباب البريطانيين المسلمين" و "مؤشرات التطرف العنيف".[209]

ويركز نمط الحوكمة الثاني على فك الاشتباك والرسائل المضادة. ويمكن استهداف الأفراد الذين يمكنهم الوصول بالفعل إلى المحتوى المتطرف على الإنترنت واستخدامه بروايات مضادة تقدم "تفسيرات بديلة صادقة لهذا العالم وحسن توجيه للصلاحيات والتعامل مع ما تروجه الجماعات المتطرفة العنيفة" بإعادة تأكيد روح التسامح والمصارحة والحرية والديمقراطية.[210] وفيما يتعلق بمنصات المراسلة الفورية مثل تليغرام، فقد ينطوي ذلك على تسلل القنوات والجماعات لنشر روايات بديلة على أمل إبعاد بعض الأفراد عن الراديكالية.

وفيما تمتاز الرسائل المضادة بإمكاناتها، تفتقر الاتصالات الإستراتيجية التي تقودها الحكومة إلى الفعالية إلى حد كبير،[211] وترتبت عليها عواقب سلبية غير مقصودة. وأثار برنامج Think Again Turn Away التابع لوزارة الخارجية الأمريكية غضبًا وردود فعل عنيفة عند نشر رسائل مضادة والدخول في نزاعات على تويتر مع حسابات تابعة

---

207 UK Home Office, 'Counter-Terrorism Strategy: The Four Ps: Pursue, Prevent, Protect, Prepare'. متاح عبر: https://web.archive.org/web/20090711105017/http://security.homeoffice.gov.uk/counter-terrorism-strategy/about-the-strategy1/four-ps/;
HM Government, 'CONTEST: The United Kingdom's Strategy for Countering Terrorism'، يونيو 2018. متاح عبر: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf

208 Dodd, V. 'Government anti-terrorism strategy "spies" on innocents,' The Guardian، 16 أكتوبر 2009. متاح عبر: https://www.theguardian.com/uk/2009/oct/16/anti-terrorism-strategy-spies-innocents

209 Abbas, T. (2019) 'Implementing "Prevent" in Countering Violent Extremism in the UK: A Left-Realist Critique,' Critical Social Policy 39, no. 3: pp. 396–412

210 Waldman, S. & Verga, S. (2016) 'Countering violent extremism on social media,' Centre for Security Science, Defence Research and Development Canada, p.7. متاح: https://cradpdf.drdc-rddc.gc.ca/PDFS/unc262/p805091_A1b.pdf

211 Bartlett, J. & Krasodomski-Jones, A. (2015) 'Counter-Speech: examining content that challenges extremism online,' Demos. متاح: https://www.demos.co.uk/wp-content/uploads/2015/10/Counter-speech.pdf

ومؤيدة لتنظيم داعش.[212] وتوصلت الأبحاث التي أجرتها Demos إلى أن إجمالي المشاركات التي حققتها الصفحات الأوروبية المعارضة للتعبير على فيسبوك لا يزال دون المستوى.[213] وتفتقر مبادرات التواصل الاستراتيجي التي تدعمها الحكومة إلى المصداقية بسبب ما يسمى بفجوة "قُل-افعل"، وتعني أن رسالة التطرف العنيف تصبح أقوى كلما اتسعت الفجوة بين القيم التي تروجها الحكومات وأفعالها.[214]

لذا، كثيرًا ما تخفف الجهود اللاحقة في مبادرات الرسائل المضادة عبر الإنترنت التركيز على أهمية المشاركة الحكومية، ويأخذ بزمامها أرباب هذه الصناعة. وحققت غوغل وشركتها الأم، Alphabet، الريادة في استخدام "طريقة إعادة توجيه المحتوى" التي تستهدف متصفحي محتوى تنظيم داعش عبر الإنترنت وتعيد توجيههم إلى مقاطع فيديو منسقة على YouTube تعارض رسائل التطرف العنيف.[215] يطرح محتوى الفيديو المنسق على المستضعفين والراديكاليين روايات تشدد على قيم التسامح والتنوع والشمولية وغيرها. وحققت شركة Alphabet ريادتها في استخدام طريقة إعادة توجيه المحتوى من خلال شريكها الرائد Moonshot CVE الذي يدير حملات رسائل مضادة بخمس عشرة لغة في أكثر من ثماني وعشرين دولة.[216] وتعاونت رابطة مكافحة التشهير (Anti-Defamation League)، التي تتخذ من الولايات المتحدة مقراً لها، مع Moonshot CVE لمواجهة النشاط العنصري الأبيض والجهادي على الإنترنت.[217]

ومع أن جهود Moonshot CVE يمكنها تقويض مسيرة الراديكالية، فإن الحلول التي تقودها الصناعة للمشاكل الاجتماعية والسياسية لها تحدياتها. وشركة Moonshot CVE مستقلة وبعيدة عن طائلة الرقابة أو المساءلة الحكومية أو المجتمع المدني. ولا تفصح الشركة عن أي بيانات إلا إذا كانت عالية المستوى وتتعلق بعملياتها، ولم تتضح الأسباب التي دعتها لاختيار إعادة التوجيه أو الكيفية التي تم بها.[218]

ويأتي نمط الحوكمة الثالث – تنظيم المنصات – في نهاية عملية الراديكالية. وفي التقرير أعلاه، يتناول كليفورد الجهود التي تبذلها جهات إنفاذ القانون للضغط على منصات مثل تليغرام للامتثال لأوامر المحكمة بشأن الاشتباه في نشاط إرهابي. وعلى سبيل المثال، في الصفحة 5، استعرض كليفورد أيام إجراءات إحالة اليوروبول التي حملت تليغرام على تحديث سياسة خصوصيتها بأن تتضمن بندًا يجيز للمنصة عرض بيانات المستخدم على السلطات المختصة لتحديد هويته عند الاشتباه في تطرف المحتوى. وتعاونت المنصات الأخرى التي ورد ذكرها بالتفصيل في التقرير أعلاه بدرجات متفاوتة مع الحكومات ووكالات إنفاذ القانون لمكافحة انتشار المحتوى المتطرف.

ومن التحديات التي يفرضها هذا النمط من الحوكمة أن مشاركة صانعي السياسات ووكالات إنفاذ القانون في هذه الجهود التنظيمية "كالحرث في الماء": بمجرد موافقة المنصة على التعاون مع أوامر المحكمة، تظهر منصة بديلة أخرى في مكانها لحماية خصوصية المستخدمين. ويخلص التقرير إلى أنه "مع ظهور منصات المراسلة الفورية التي يتزايد استقرارها وتقدم ميزات جديدة لتعزيز الخصوصية والأمان، يتساءل المتطرفون، الذين ينتقلون من تليغرام إلى برنامج ثانوي للمراسلة الفورية، «متى» و «ماذا»، وليس «لو».“

والنهج الذي يرتكز على الميزات في مكافحة التطرف عبر الإنترنت، كما هو موضح في الصفحات الأخيرة من التقرير أعلاه، يفتح الباب لإمكانية التوصل إلى صورة جديدة من صور الحوكمة غير النُهج الثلاثة الموضحة هنا. ويعتمد كل نمط من الأنماط المذكورة أعلاه على الحوكمة الرأسية من أعلى إلى أسفل، وغالبًا ما تتولاها مؤسسات الدولة بالاستناد إلى مبررات تشريعية.[219] وتشارك الوقاية المبكرة والرسائل

212 Katz, R. (2014) 'The State Department's Twitter War with ISIS is Embarrassing,' Time. متاح: https://time.com/3387065/isis-twitter-war-state-department/

213 Bartlett & Krasodomski-Jones, 'Counter-Speech'

214 Romaniuk, P. (2015) 'Does CVE Work? Lessons Learned from the Global Effort to Counter Violent Extremism,' Global Center on Cooperative Security. متاح: https://www.globalcenter.org/wp-content/uploads/2015/09/Does-CVE-Work_2015.pdf, p.33

215 انظر: https://redirectmethod.org/

216 انظر: http://moonshotcve.com/work/

217 'ADL and Partners Counter White Supremacists Online Through Google Search,' Anti-Defamation League. متاح: https://www.adl.org/news/press-releases/adl-and-partners-counter-white-supremacists-online-through-google-search

218 انظر: http://moonshotcve.com/work/

219 Zwitter, A. & Hazenberg, J. (2020), 'Decentralized Network Governance: Blockchain Technology and the Future of Regulation,' Frontiers in Blockchain. متاح عبر: https://www.frontiersin.org/articles/10.3389/fbloc.2020.00012/full

المضادة والقواعد التنظيمية في هيكلٍ لحوكمة "القيادة والسيطرة" تستعين به الكيانات (الحكومات والشركات وجهات إنفاذ القانون ووكالات الاستخبارات) في وضع سياساتها وتوجيهها لأسفل.

وقد تحتاج الشبكة اللامركزية، التي تحددها ميزاتها المقدمة للمستخدمين، إلى نمط حوكمة تغلب عليه اللامركزية. وبدلاً من هيكل الحوكمة الرأسي، قد تتحقق النتيجة المنشودة في صنع السياسات باتباع نهج أفقي يحاكي هيكل الإنترنت اللامركزي. وتُعد المبادرات المتعددة القطاعات، مثل التوسع في منتدى الإنترنت العالمي لمكافحة الإرهاب (GIFCT)، على حد وصف كليفورد في الصفحة 22 أعلاه، التي تجمع أعدادًا أكبر من مقدمي الخدمات بصانعي السياسات والخبراء الأكاديميين، مثالاً جيدًا على اتباع نهج تغلب عليه اللامركزية.

ومن التوصيات التي وردت في تقرير سابق أصدرته الشبكة العالمية للتطرف والتكنولوجيا (GNET)، الذكاء الاصطناعي ومكافحة التطرف العنيف، أن تعديل المحتوى الضار عبر الإنترنت سيكون فعالاً للغاية إذا كُلفت به هيئة تنظيمية مستقلة.[220] ومشاركة المجتمع المدني والحكومة والصناعة ومقدمي الخدمات في وضع القواعد التنظيمية، تحت إشراف هيئة مستقلة ومتعددة الجنسيات، سوف تطرح نمطًا شموليًا لحوكمة مكافحة التطرف العنيف يغلب عليه الطابع الأفقي. ويمكن بالفعل هيكلة هذه الهيئة وربطها بميزات المنصات اللامركزية والمحتوى المتطرف العنيف عبر الإنترنت، كما يقترح كليفورد أعلاه، وذلك بهدف "التحضير الاستباقي للاستجابة ... [و] تقويض تبني المتطرفين منصات جديدة." ويستطيع هذا النمط اللامركزي للحوكمة أن يحقق فعالية كبيرة في التكيف مع تحديات التحول نحو الإنترنت اللامركزي ومواجهة هذه التحديات.

220 الشبكة العالمية للتطرف والتكنولوجيا (GNET)، "الذكاء الاصطناعي ومكافحة التطرف العنيف: كتاب تمهيدي"، ص 41. متاح عبر: https://gnet-research.org/wp-content/uploads/2020/09/GNET-Report-Artificial-Intelligence-and-Countering-Violent-Extremism-A-Primer_ARABIC.pdf

Global Network
on Extremism & Technology

بيانات الاتصال

لأي أسئلة أو استفسارات، أو للحصول على نسخ أخرى من هذا التقرير، يرجى التواصل مع:

ICSR
King's College London
Strand
London WC2R 2LS
المملكة المتحدة

هاتف: +44 20 7848 2098
بريد إلكتروني: mail@gnet-research.org

تويتر: @GNET_research

هذا التقرير، كغيره من منشورات الشبكة العالمية للتطرف والتكنولوجيا (GNET)، يمكن تنزيله مجانًا من موقع شبكة GNET على الإنترنت www.gnet-research.org.