Global Network
on Extremism & Technology

Instants migratoires : adoption des applications de messagerie instantanée par les groupes extrémistes

Bennett Clifford

Le GNET est un projet spécial du Centre international d'étude de la radicalisation du King's College, à Londres.

L'auteur de ce rapport est Bennett Clifford, chercheur principal au sein du Programme sur l'extrémisme de l'Université George Washington.

Le Global Network on Extremism and Technology (Réseau mondial sur l'extrémisme et la technologie – GNET) est une initiative de recherche universitaire bénéficiant du soutien du Forum mondial de l'Internet contre le terrorisme (GIFCT), une initiative indépendante mais financée par le secteur qui vise à mieux comprendre et lutter contre l'utilisation des technologies par les groupes terroristes. Le GNET est formé et dirigé par le Centre international d'étude de la radicalisation (ICSR), un centre de recherche universitaire basé dans les locaux du Département d'étude des guerres du King's College, à Londres. Les opinions et conclusions exprimées dans ce document sont celles des auteurs et ne doivent en aucun cas être interprétées comme représentant les opinions et conclusions, expresses ou implicites, du GIFCT, du GNET ou de l'ICSR.

COORDONNÉES

Pour toute question, demande d'information et demande de copies supplémentaires du présent rapport, contacter :

ICSR
King's College London
Strand
Londres WC2R 2LS
Royaume-Uni

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter : **@GNET_research**

Ce rapport peut, comme toutes les autres publications du GNET, être téléchargé gratuitement à partir du site Internet du GNET : www.gnet-research.org.

Résumé exécutif

- Les extrémistes de tous bords – y compris les partisans djihadistes d'al-Qaïda et de l'État islamique en Syrie et en Irak et différents groupes d'extrême droite – utilisent aujourd'hui l'application de messagerie instantanée Telegram comme forum de coordination central de leurs activités en ligne. Cependant, compte tenu des nouvelles politiques de cette dernière, de sa collaboration avec les forces de l'ordre et d'autres partenaires du secteur, et du renforcement de l'application de ses conditions d'utilisation, les extrémistes commencent à ressentir une pression importante pesant sur l'écosystème qu'ils ont construit autour de Telegram.

- Les djihadistes et partisans d'extrême droite connectés testent constamment, parallèlement à Telegram, d'autres applications de messagerie instantanée pouvant servir de solutions de rechange. La transition à grande échelle vers une autre plateforme est toutefois improbable à court terme. L'ensemble de fonctionnalités de Telegram, la connaissance approfondie qu'en ont les extrémistes et sa facilité d'utilisation par rapport à la concurrence garantissent que l'exploitation de cette plateforme par les extrémistes est susceptible de se poursuivre malgré les nouveaux régimes d'application des lois de l'entreprise.

- Parallèlement aux difficultés que connaissent les sympathisants des groupes extrémistes pour rester sur Telegram, certains groupes ont essayé ou prévoient d'établir une présence sur d'autres applications de messagerie instantanée. Ainsi, ces deux dernières années, six plateformes (BCM, Gab Chat, Hoop Messenger, Riot.im, Rocket.Chat et TamTam) ont été envisagées par les groupes extrémistes pour remplacer Telegram.

- Dans cette analyse, nous montrons que les extrémistes ont gravité vers ces plateformes en raison des fonctionnalités proposées, de leur facilité d'utilisation et des positions des entreprises les ayant créées sur la confidentialité, la sécurité et la régulation des contenus extrémistes.

- Deux tendances concernant l'exploitation des applications de messagerie instantanée par les groupes extrémistes devraient se dégager à l'avenir :

    - Les partisans des groupes extrémistes ayant établi une présence importante sur Telegram sont susceptibles de rechercher des plateformes proposant des fonctionnalités, potentialités et présentations visuelles similaires à celles de Telegram.

    - Les partisans des groupes extrémistes sont également susceptibles de poursuivre leurs efforts visant à exploiter des plateformes de messagerie instantanée proposant l'utilisation de serveurs et un stockage des données décentralisés.

- Pour lutter contre l'exploitation des applications de messagerie instantanée par les groupes extrémistes, plusieurs initiatives sectorielles conjointes, comme le Forum mondial de l'Internet contre le terrorisme (GIFCT), envisageront peut-être d'intégrer les fournisseurs de services de messagerie instantanée dans les forums individuels de collaboration et de partage d'informations. Plus généralement, les chercheurs, décideurs politiques et professionnels de la lutte contre l'extrémisme en ligne devraient réfléchir à une approche fondée sur les fonctionnalités, plutôt que sur les plateformes, pour évaluer l'exploitation des technologies de communication numérique par les groupes extrémistes.

Table des matières

1 Introduction : extrémistes, Telegram et transition

Ce rapport examine les nombreuses applications de messagerie instantanée en ligne privilégiées par les groupes djihadistes et d'extrême droite, en recensant leurs potentialités techniques et le positionnement des entreprises sur le respect de la vie privée des utilisateurs, la sécurité et la régulation des contenus. À cette fin, nous analyserons ici six services de messagerie en ligne (BCM, Gab Chat, Hoop Messenger, Riot.im, Rocket.Chat et TamTam) qui ont été ou sont susceptibles d'être utilisés par les groupes extrémistes parallèlement à Telegram.

Actuellement, de nombreux sympathisants de différents groupes extrémistes se concentrent sur le service de messagerie instantanée en ligne Telegram, même si certains font des incursions sur d'autres plateformes[1]. L'application Telegram est régulièrement désignée comme la « plateforme de choix » des djihadistes en ligne, en particulier des partisans de l'État islamique en Irak et en Syrie (EI), mais a également toujours été très populaire auprès des mouvements d'extrême droite[2]. Les analystes et chercheurs spécialisés dans l'extrémisme en ligne, de même que de nombreux gouvernements, considèrent Telegram comme une plateforme de communication stable pour les groupes extrémistes de tous bords en raison de l'ensemble de ses fonctionnalités, y compris les communications chiffrées de bout en bout et ses garanties d'anonymat et de respect de la vie privée[3]. Les extrémistes utilisent les chaînes et groupes Telegram comme bases arrières pour instaurer une « tendance multiplateforme », où les contenus médiatiques sont rediffusés de Telegram vers d'autres plateformes de messagerie et sites Internet destinés au public[4].

Les modifications apportées récemment par Telegram à ses conditions d'utilisation et à sa politique de confidentialité affaiblissent toutefois les potentialités offertes par la plateforme aux groupes extrémistes. Par exemple, en avril 2018, Telegram a ajouté une Section 8.3 à sa politique de confidentialité. Celle-ci marque une rupture avec l'ancien moratoire de Telegram relatif au partage d'informations avec les gouvernements : elle dispose que « si Telegram reçoit une ordonnance judiciaire confirmant que vous êtes soupçonné(e) de terrorisme, nous nous réservons le droit de communiquer votre adresse IP et votre numéro de téléphone aux autorités compétentes »[5]. Parallèlement à la modification de sa

1 Clifford, Bennett, et 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 ; Mia Bloom, Hicham Tiflati et 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 ; Mia Bloom et Chelsea Daymon. 2018. « Assessing the Future Threat: ISIS's Virtual Caliphate ». Orbis 62 (mai). https://doi.org/10.1016/j.orbis.2018.05.007 ; « Telegram: The Latest Safe Haven for White Supremacists ». 2019. Anti-Defamation League. 2 décembre 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 et Powell, « Encrypted Extremism ».

4 *Ibid.*

5 *Ibid.*

politique de confidentialité, l'application a également commencé à participer à des « journées d'action de signalement »[6]. Lors de la onzième journée d'action de signalement, la participation de Telegram se résumait à observer le processus de détection et d'identification des contenus à caractère terroriste mis en place par les forces de l'ordre européennes[7]. Lors de la seizième journée d'action de signalement en novembre 2019, toutefois, Telegram a collaboré avec Europol et ses partenaires du secteur Google, Twitter et Instagram[8]. Les plateformes ont conjointement supprimé 26 000 éléments de propagande de l'EI au total, y compris des comptes, des chaînes, des groupes, des vidéos et d'autres publications de leurs sites[9]. Le porte-parole du parquet fédéral belge, Eric Van Der Sypt, s'est exprimé sur ces actions, affirmant que grâce aux suppressions de masse, l'EI n'était, pour l'heure, « plus présent sur Internet »[10].

Malgré l'évaluation initiale de Van Der Sypt, les groupes extrémistes ont maintenu leur présence sur Telegram après les journées d'action de signalement. Si l'opération a porté un coup temporaire aux partisans de l'EI présents sur Telegram, les analyses du Global Network on Extremism and Technology (Réseau mondial sur l'extrémisme et la technologie – GNET) ont montré que le service comptait encore des « vestiges tenaces de sa présence » et que la « diffusion de propagande officielle et non officielle se poursuivait à un rythme régulier[11]. Les sympathisants de l'EI, le seul groupe reconnu comme ayant été ciblé par l'effort, ont rapidement assuré leur présence sur plusieurs autres plateformes de messagerie instantanée en ligne. Grâce à la décentralisation, ils ont pu rester en ligne, la « dispersion vers ces dizaines de plateformes ayant renforcé la décentralisation de la diffusion de propagande djihadiste », et l'EI a « étendu sa portée » en diffusant ses contenus un peu partout sur la toile[12]. En juillet 2020, une évaluation Europol a déclaré que « les efforts pour établir la présence de l'EI en ligne se poursuivent sur plusieurs plateformes, y compris Telegram »[13]. Les agents responsables des journées d'action de signalement de Telegram ont remarqué que les efforts portaient principalement sur les partisans de l'EI, laissant d'autres groupes djihadistes et d'autres groupes extrémistes violents relativement à l'abri de ces mesures de répression[14].

Alors que les mesures de suppression des contenus de l'EI battaient leur plein sur Telegram, les groupes d'extrême droite ont maintenu leur forte présence sur la plateforme, aucunement gênés par les

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 octobre 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 novembre 2019. https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online.
9 *Ibid*.
10 Zialcita, Paolo. 2019. « Islamic State 'Not Present On The Internet Anymore' Following European Operation ». NPR.Org. 25 novembre 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. Global Network on Extremism and Technology. 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. Global Network on Extremism and Technology. 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 janvier 2020. https://www.flashpoint-intel.com/blog/terrorism/jihadists-presence-online-decentralizes-after-telegram-ban/.
13 « Online terrorist propaganda: 2019 in Review." 2020. Europol. 28 juillet 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 ».

efforts de suppression de contenu[15]. Pourtant, cette dynamique pourrait bien être en train de changer. Cet été, Telegram a coordonné des actions de retrait de contenu de masse des chaînes et groupes d'extrême droite sur sa plateforme[16]. L'application a suspendu certaines des chaînes les plus violentes et les plus virulentes des groupes d'extrême droite, y compris Terrorwave Refined, une « plateforme centrale » de l'extrême droite violente sur Telegram, ainsi que des chaînes liées à la Misanthropic Division et à RapeKrieg[17]. Malgré ces suppressions, la plupart des chaînes d'extrême droite sur Telegram demeurent intactes, et les administrateurs des chaînes supprimées poursuivent leurs efforts pour publier leurs contenus sur la plateforme[18]. Reste à voir si les groupes d'extrême droite présents sur Telegram vont sérieusement envisager l'utilisation d'une autre plateforme ou si les efforts de Telegram vont véritablement se poursuivre.

15 Katz, Rita. 2020. « Neo-Nazis Are Running Out of Places to Hide Online ». WIRED, 9 juillet 2020. https://www.wired.com/story/neo-nazis-are-running-out-of-places-to-hide-online/.
16 *Ibid.*
17 *Ibid.*
18 *Ibid.*

2 Applications de messagerie instantanée : catégories d'analyse

Un retrait total de Telegram des groupes extrémistes et une migration de masse vers une autre plateforme est peu probable à court terme. Mais nous devons appréhender les autres plateformes de messagerie qu'ils utilisent parallèlement à Telegram. Les extrémistes ne décident pas d'utiliser l'une ou l'autre plateforme ; ils en exploitent généralement plusieurs à la fois[19]. Tous comme ils ont effectué des tests sur Telegram alors que Twitter et Facebook étaient encore des plateformes globalement accueillantes, ils sont susceptibles de tester des plateformes de messagerie secondaires même tant que l'application Telegram reste engageante. Par ailleurs, l'analyse comparée de ces plateformes secondaires et de Telegram peut aider à déterminer les types de caractéristiques des plateformes de messagerie les plus attrayants pour les groupes extrémistes. En supposant que Telegram continue de déployer des efforts considérables et vigoureux pour chasser les extrémistes de ses plateformes, il est nécessaire pour les professionnels de comprendre les plateformes de second plan afin de contenir les effets secondaires des campagnes de suppression, comme la migration des extrémistes vers les plateformes moins réglementées leur offrant plus de potentialités ou des politiques de confidentialité et de sécurité bloquant l'accès des forces de l'ordre, des services de renseignement ou des plateformes elles-mêmes aux messages extrémistes.

Les six plateformes présentées dans cette analyse ne constituent bien évidemment pas une liste exhaustive des messageries instantanées utilisées par les groupes extrémistes à l'heure actuelle. Elles ont cependant toutes dû faire face à une exploitation de leurs services par des groupes extrémistes ces dernières années ; les comparaisons entre plateformes peuvent aider à dégager certaines potentialités fondamentales jouant un rôle important dans le choix effectué par ces groupes. Plus spécifiquement, ce rapport examine, pour chacune d'entre elles, cinq facteurs pouvant définir leur position globale vis-à-vis des contenus à caractère extrémiste : utilisation par les groupes extrémistes, ensembles de fonctionnalités, accessibilité par les utilisateurs, confidentialité et sécurité, et contexte politique/réglementaire. Chacune de ces catégories comporte plusieurs questions fondamentales sur l'usage des plateformes de messagerie instantanée par les groupes extrémistes :

- *Utilisation par les groupes extrémistes :* Quels types de groupes extrémistes utilisent la plateforme ? Quand ont-ils commencé à l'utiliser ? L'utilisent-ils à l'heure actuelle ? Quelle est l'étendue de l'utilisation de la plateforme par les groupes extrémistes ?

19 Prucha, « IS and the Jihadist Information Highway » ; Alkhouri, Laith, et 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.

- *Ensemble de fonctionnalités :* Quelles fonctionnalités la plateforme propose-t-elle ? Parmi elles, laquelle/lesquelles la distingue(nt) de ses concurrentes, notamment lorsqu'il s'agit de son utilisation (abusive) par les groupes extrémistes ?

- *Accessibilité par les utilisateurs :* Est-il facile d'utiliser la plateforme ? Que faut-il faire pour créer un compte et accéder à des contenus spécifiques ? Quels protocoles le système exploite-t-il pour fonctionner ? La plateforme subit-elle des perturbations, des tentatives de piratage ou d'autres efforts de déni de service ?

- *Confidentialité et sécurité :* Que stipulent les conditions d'utilisation de la plateforme à propos de la vie privée des utilisateurs ? La plateforme propose-t-elle un chiffrement des données ? Où stocke-t-elle les données des utilisateurs ? Quels tiers peuvent avoir accès à ces données ?

- *Contexte politique/réglementaire :* Quelle est la politique de la plateforme en matière de suppression de contenu à caractère terroriste et extrémiste ? La plateforme publie-t-elle des rapports sur la transparence ? Où est-elle enregistrée, et à quelles lois sur la réglementation des contenus est-elle soumise ? Comment traite-t-elle les demandes du gouvernements relatives aux données des utilisateurs ?

Dans la dernière section, le présent rapport soulignera les fonctionnalités les plus courantes proposées par ces plateformes, afin de tenter d'analyser lesquelles sont les plus attrayantes pour les groupes extrémistes. Nous défendrons également l'adoption d'une approche fondée sur les fonctionnalités, et non sur les plateformes, pour analyser et lutter contre l'utilisation d'Internet par les groupes extrémistes.

3 Utilisation d'applications de messagerie instantanée secondaires par les groupes extrémistes

Cette section analyse six plateformes de messagerie instantanée exploitées par les extrémistes, ou susceptibles de l'être, en raison du renforcement de l'application des conditions d'utilisation de Telegram. Six mois après les journées d'action de signalement auxquelles a participé l'application, un rapport d'Europol a conclu qu'après une vague de suppression de contenus, les djihadistes affiliés à l'EI présents en ligne « ont afflué vers TamTam et Hoop Messenger » tout en testant d'autres « applications marginales comme la messagerie blockchain BCM, RocketChat et le logiciel gratuit de messagerie instantanée Riot »[20]. Leurs homologues dans d'autres groupes djihadistes, de même que les groupes d'extrême droite, ont eux aussi lancé leurs propres expérimentations sur plusieurs de ces plateformes. Nous analyserons dans cette section une sixième plateforme, Gab Chat, aujourd'hui en cours de développement mais susceptible d'attirer les groupes d'extrême droite compte tenu de ses potentialités et de l'historique de l'entreprise hôte[21].

BCM Messenger

BCM (Because Communication Matters) Messenger était une application décentralisée de messagerie qui offrait des services de conversation privée et de groupe à plus de 100 000 participants[22]. Si les origines de l'entreprise sont obscures, la plateforme a été créée par des développeurs chinois et enregistrée dans les îles Vierges britanniques comme alternative décentralisée à la plateforme chinoise de messagerie WeChat[23]. Plusieurs observateurs des médias extrémistes en ligne ont remarqué que les partisans de l'EI testaient de plus en plus cette application au lendemain des journées d'action de signalement de 2019[24]. Par exemple, l'un des principaux réseaux de médias en ligne affiliés à l'EI, Nashir News Agency,

20 Europol, « Online Jihadist Propaganda: 2019 in Review ».
21 Morse, Jack. 2020. « Police are worried about white extremists organizing on Gab Chat, leaked documents show ». 13 juillet 2020. https://mashable.com/article/law-enforcement-documents-violent-white-extremists-encrypted-gab-chat/.
22 « BCM Messenger ». n.d. BCM Messenger. Consulté le 1er avril 2020. « Politique de confidentialité ». n.d. BCM Messenger. Consulté le 1er avril 2020. Le service BCM n'existe plus. Des versions accessibles de la page et de la politique de confidentialité de BCM sont disponibles via Wayback Machine, à l'adresse suivante : https://web.archive.org/web/20200215082731/https://bcm.social/index.html et https://web.archive.org/web/20191016053505/https://bcm.social/license/policy.html.
23 *Ibid.* ; Yuan, Lanny, Huaibing Jian, Peng Liu, Pengxin Zhu et ShanYang Fu. 2018. « AME Blockchain: An Architecture Design for Closed-Loop Fluid Economy Token System ». Livre blanc.
24 Smith, Brenna. 2019. « Terrorists Use a New Blockchain Messaging App after Telegram Crackdown ». Bellingcat CryptOSINT. 10 décembre 2019. https://mailchi.mp/7884c14d5fb9/terrorists-use-a-new-blockchain-messaging-app-after-telegram-crackdown.

a créé plusieurs chaînes sur la plateforme en décembre 2019[25]. En février 2020, l'entreprise a informé ses utilisateurs qu'elle mettait un terme à son service de messagerie[26].

BCM se distinguait de Telegram et d'autres messageries instantanées en ligne à plusieurs égards. D'abord et avant tout, l'application fonctionnait sur un modèle de serveur décentralisé. Contrairement aux autres services de messagerie, qui stockent les informations et données des utilisateurs sur des serveurs centralisés contrôlés par le prestataire, BCM et d'autres plateformes décentralisées ont réparti les points du serveur sur le réseau des utilisateurs, permettant ainsi à chacun d'entre eux de stocker et de contrôler l'accès à leurs propres données[27]. Si certaines messageries instantanées en ligne fournissent un chiffrement de bout en bout pour certaines (mais pas toutes) formes de communication ou ne le fournissent que sur demande, les messages envoyés via BCM étaient chiffrés par défaut[28]. Autrement, l'ensemble de fonctionnalités (conversations privées et de groupe) et l'algorithme de chiffrement utilisé par BCM étaient comparables à ceux de Telegram[29].

Pour créer un compte sur BCM, les utilisateurs potentiels pouvaient simplement télécharger l'application et saisir un identifiant utilisateur. Contrairement à Telegram, il n'était pas nécessaire d'avoir un numéro de téléphone pour s'enregistrer[30]. L'accès à certains groupes nécessitait un URL vers le contenu et la communication directe avec d'autres utilisateurs supposait de connaître leur clé publique ou leur identifiant utilisateur BCM. BCM était basé sur une « plateforme d'infrastructure et d'application décentralisée » appelée AME, construite sur un principe de « confiance zéro » : « l'appli BCM ne fait confiance à personne d'autre qu'elle même, pas même au serveur BCM »[31]. Personne, y compris le serveur BCM lui-même, n'était capable de déchiffrer les messages envoyés entre utilisateurs. BCM propose également un portefeuille de cryptomonnaie en parallèle de son service de messagerie instantanée, qui existe encore aujourd'hui malgré la fermeture du service de messagerie[32]. D'aucuns ont par conséquent affirmé, à tort, que le service de messagerie instantanée était « basé sur la technologie blockchain », même si seul l'était le portefeuille numérique[33].

D'après la politique de confidentialité de BCM, l'entreprise « n'utilisera ni ne communiquera [les données des utilisateurs] à des tiers sans autorisation préalable »[34]. Sa plateforme décentralisée et son offre de chiffrement de bout en bout par défaut de toutes les communications empêchait l'entreprise de déchiffrer les messages entre utilisateurs. Les données de ces derniers étant stockées par des nœuds individuels dans le réseau, les demandes d'accès aux serveurs émises par les forces de l'ordre auraient été difficiles à honorer[35]. L'entreprise n'a

25 *Ibid.* ; *Flashpoint, « Jihadists Presence Online Decentralizes After Telegram Ban » ; Gluck, « Islamic State Adjusts Strategy to Remain on Telegram » ; Webb, Sam, et Colin Rivet. 2019. « Terror Group ISIS Testing Blockchain Messaging App ». 16 décembre 2019.* https://finance.yahoo.com/news/terror-group-isis-testing-blockchain-150028142.html.
26 Message aux abonnés BCM, 22 février 2020. https://postimg.cc/3dWTwGmp.
27 Yuan *et al.*, « AME Blockchain: An Architecture Design for Closed-Loop Fluid Economy Token System ».
28 « FAQ ». n.d. BCM Messenger. Consulté le 1er avril 2020. https://web.archive.org/web/20200115224708/https://bcm.social/faq.html.
29 *Ibid.*
30 *Ibid.*
31 *Ibid.*
32 *Ibid.*
33 *Ibid.*
34 BCM Messenger, « Politique de confidentialité ».
35 *Ibid.*

pas communiqué sur la façon dont elle prévoyait de lutter contre les contenus à caractère terroriste ou extrémiste, mais l'un de ses porte-paroles a indiqué que si elle comptait respecter les lois à l'échelle locale, elle ne comptait « en aucun cas répondre favorablement aux demandes de fourniture d'accès dissimulé ou de services de déchiffrement visant à surveiller les contenus des utilisateurs »[36].

Gab Chat

Gab est un site créé en 2016 comme une « alternative respectueuse de la liberté d'expression » à Twitter ; son cofondateur, Andrew Torba, a justifié sa création par l'existence d'un « monopole gauchiste des réseaux sociaux »[37]. Gab a gagné en notoriété en tant que point névralgique en ligne pour l'extrême droite, et attiré beaucoup attention lorsqu'il a été constaté que l'auteur de la fusillade survenue en octobre 2018 dans la synagogue Tree of Life, à Pittsburgh, faisait partie d'une communauté néonazie à la marge sur cette plateforme[38]. Depuis, plusieurs prestataires de services ont cessé de fournir des services à Gab[39]. Après être passé d'un hébergeur de services à un autre, Gab a conservé plus d'un million de comptes et une communauté stable de partisans d'extrême droite[40].

Fin janvier 2020, Gab a annoncé qu'il était dans les premiers stades de développement d'une plateforme de messagerie instantanée similaire à Telegram, appelée Gab Chat[41]. Le service est décrit comme un « service de messagerie par chat chiffré comprenant des espaces de discussion publics et privés »[42]. Torba a déclaré que, tout comme pour Telegram, les espaces de discussion publics n'offriraient pas le chiffrement par défaut de toutes les communications, mais que les discussions privées seraient, elles, chiffrées de bout en bout : « les espaces chiffrés ne pourront pas être lus par des personnes extérieures à l'espace de discussion, pas même Gab »[43]. De plus, l'application Gab Chat ne serait hébergée que sur le site Internet de Gab et non sur les boutiques d'applications populaires proposées par Google et Apple[44].

Le principal avantage de la plateforme Gab pour les extrémistes est la garantie fournie par l'entreprise que les contenus ne seraient ni modérés ni supprimés. Celle-ci considère la liberté d'expression comme un principe inviolable, et est fière de sa politique contre la censure[45]. Toutefois, « si une menace illicite est détectée sur la plateforme ou si nous apprenons qu'un individu susceptible d'avoir créé un compte sur notre site a eu une conduite violente grave hors plateforme », l'entreprise « [coopérera] et [communiquera] fréquemment

36 *Ibid.*
37 Lorenz, Taylor. 2018. « The Pittsburgh Suspect Lived in the Web's Darkest Corners ». The Atlantic. 27 octobre 2018. https://www.theatlantic.com/technology/archive/2018/10/what-gab/574186/.
38 *Ibid.*
39 Jurecic, Quinta. 2018. « Gab Vanishes, and the Internet Shrugs ». Lawfare. 29 octobre 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 mars 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 janvier 2020. https://news.gab.com/2020/01/31/ag-barr-is-wrong-on-encryption-introducing-gab-chat-our-open-source-encrypted-messaging-platform/.
42 *Ibid.*
43 *Ibid.*
44 *Ibid.*
45 Torba, Andrew. 2019. « Gab's Policies, Positions, and Procedures for Unlawful Content And Activity On Our Social Network ». Gab News (blog). 23 août 2019. https://news.gab.com/2019/08/23/gabs-policies-positions-and-procedures-for-unlawful-content-and-activity-on-our-social-network/.

avec les forces de l'ordre fédérales, locales et étatiques (…) pour participer à la prohibition des formes graves de criminalité »[46].

Gab Chat existe encore en version beta[47]. Compte tenu de sa popularité chez les partisans d'extrême droite comme alternative aux prestataires de réseaux sociaux publics comme Twitter et Facebook cependant, il est raisonnable de supposer que l'application sera adoptée par des groupes extrémistes. À cela s'ajoute la popularité de Telegram et de services similaires parmi les sympathisants d'extrême droite. Si Gab Chat fournit des services comparables à ceux proposés par Telegram sous la bannière Gab, les partisans d'extrême droite pourront la considérer comme une plateforme de messagerie instantanée accueillante et tenter de l'exploiter lorsqu'elle sera pleinement fonctionnelle.

Hoop Messenger

Hoop Messenger est une application de messagerie instantanée en ligne qui, à l'instar de Telegram, fournit des solutions de communication sous forme de conversations privées, d'espaces de discussion et de chaînes à distribution multiple. Le service est géré par une petite entreprise installée au Canada[48]. En décembre 2019, après les efforts de suppression de médias liés à l'EI coordonnés par Europol, plusieurs médias officiels et non officiels de l'EI et d'al-Qaïda ont créé des chaînes sur Hoop Messenger, certains partisans encourageant l'utilisation de la plateforme comme une alternative sécurisée à Telegram[49]. Quelques jours plus tard toutefois, l'entreprise a supprimé un grand nombre de chaînes connectées à l'EI de sa plateforme[50]. Fin janvier 2020, une fondation médiatique pro-EI a alerté ses abonnés contre l'utilisation de Hoop Messenger, en déclarant que l'application recueillait beaucoup d'informations personnelles sur ses utilisateurs[51].

L'EI maintient, encore aujourd'hui, une présence importante sur Hoop Messenger. Du point de vue de certains partisans importants de l'EI, cette application demeure la solution la plus attrayante pour remplacer Telegram. Début juin 2020, l'agence Nashir News Agency a publié un message « urgent » à destination de ses abonnés sur une de ses chaînes Telegram, indiquant qu'elle diffuserait désormais ses informations principalement via Hoop Messenger[52]. Cette annonce s'est inscrite dans le sillage des pressions constantes exercées sur les chaînes pro-EI par Telegram. Dans les jours qui ont suivi l'annonce, les partisans ont importé un grand nombre de chaînes pro-EI de Telegram vers Hoop Messenger[53]. La fondation Electronic Horizons, affiliée à l'EI et responsable de la production de contenus sur la sécurité numérique

46 *Ibid.*
47 Torba, « AG Barr Is Wrong On Encryption »
48 « FAQ ». n.d. Hoop Messenger. Consulté le 1er avril 2020. http://hoopmessenger.com/faq/.
49 Amarasingam, Amarnath. 2019. « Telegram Deplatforming ISIS Has Given Them Something to Fight For ». Vice. 5 décembre 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 décembre 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 décembre 2019. https://www.voanews.com/europe/struggles-regain-social-media-footing-after-europe-crackdown.
50 *Ibid.*
51 « Pro-ISIS Media Foundation Warns ISIS Supporters Against Using Hoop Messenger ». 2020. MEMRI. 27 janvier 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 ». 2020. MEMRI. 5 juin 2020. https://www.memri.org/cjlab/isis-media-outlet-announces-shift-canadian-hoop-messenger-app-after-wave-account-deletions.
53 *Ibid.*

et opérationnelle, a publié un manuel à destination de ses abonnés sur la façon d'utiliser Hoop Messenger en toute sécurité[54]. Malgré ces efforts, Hoop Messenger a riposté, lançant une autre campagne de suppression de contenu pro-EI de sa plateforme[55].

La fonction qui distingue Hoop Messenger des autres services de messagerie instantanée est son « Coffre-fort », un système de stockage de fichiers protégé par mot de passe dans lequel les utilisateurs peuvent sauvegarder des conversations, des photos, des vidéos et d'autres fichiers. Une fois créé le mot de passe, toutes les conversations et tous les fichiers sauvegardés dans le Coffre-fort sont chiffrés de bout en bout sur l'appareil de l'utilisateur et dans le cloud ; les autres chaînes et conversations ne le sont pas[56]. Les utilisateurs peuvent également créer des mots de passe pour leur Coffre-fort pouvant entraîner l'auto-destruction de son contenu lorsqu'ils sont saisis[57]. Sur le site Internet du service, les utilisateurs ont également la possibilité de supprimer leur compte à distance, ce qui efface de façon définitive toutes les données sur un compte d'utilisateur et données personnelles stockées sur leur téléphone[58]. D'après l'entreprise, les faux mots de passe et mots de passe de destruction sont particulièrement utiles lorsque « vous entrez dans des zones qui vous demandent de confier votre téléphone à quelqu'un (…). Supprimez simplement Hoop et téléchargez-le à nouveau une fois que vous récupérez votre appareil »[59].

La création d'un compte sur Hoop Messenger nécessite de s'enregistrer avec un numéro de téléphone et/ou une adresse e-mail. Contrairement à d'autres plateformes, les utilisateurs peuvent créer plusieurs identifiants utilisateurs correspondant à un même compte[60]. Les conversations ne peuvent être chiffrées de bout en bout que si l'utilisateur a choisi cette option, ce qui ne peut avoir lieu que via le Coffre-fort, mais Hoop Messenger propose un réseau privé virtuel (VPN) permettant à ses utilisateurs de naviguer le web à partir de l'application sans être contrôlés[61]. La configuration et les fonctionnalités de la plateforme sont similaires à celles de Telegram.

Les sections 9, 10 et 11 des conditions d'utilisation de Hoop Messenger précisent le positionnement du service vis-à-vis des contenus nuisibles. Le service interdit « les comportements répréhensibles et les contenus que nous jugeons inacceptables », et indique que l'entreprise supprimera tous les contenus ou comptes d'utilisateur violant les conditions d'utilisation[62]. En décembre 2019, l'entreprise a précisé que ces procédures s'appliquaient aux contenus terroristes et affirmé que l'entreprise « continuera de fermer les groupes reliés à l'EI » après avoir supprimé un nombre important de chaînes et de conversations pro-EI

54 Gluck, Raphael. 2020. « Dernière prestation d'AFAQ : un tutoriel sur l'utilisation sécurisée de Hoop Messenger, la nouvelle appli prisée par l'EI suite aux vagues de suppression de Telegram – le Magazine "The Supporters Security" sensibilise les guerriers du clavier à la sécurité – Tutoriel vidéo Debian. » Tweet, 3 juillet 2020. https://twitter.com/einfal/status/1279124715957891072.

55 Alkhouri, Laith. 2020. « De nombreuses chaînes officielles et non officielles de l'État islamique #ISIS ont été supprimées de la plateforme favorite de communication/propagande du groupe, Hoop Messenger. Cela n'a toutefois eu qu'un impact limité sur la diffusion médiatique du groupe, puisqu'il avait, très tôt, créé des dizaines de chaînes de secours. » Tweet, 6 août 2020. https://twitter.com/MENAanalyst/status/1291415487453302790.

56 Hoop Messenger, « FAQ ».

57 *Ibid.*

58 *Ibid.*

59 « Hoop Messenger ». n.d. Hoop Messenger. Consulté le 1er avril 2020. http://hoopmessenger.com/.

60 *Ibid.*

61 *Ibid.*

62 « Confidentialité et conditions ». n.d. Hoop Messenger. Consulté le 1er avril 2020. http://hoopmessenger.com/legal/.

sur la plateforme[63]. Compte tenu de l'action concertée de l'entreprise contre les contenus et comptes liés à l'EI, certains partisans semblent s'être détournés de Hoop Messenger après avoir donné l'alerte contre son utilisation[64]. D'autres sympathisants de l'EI restent néanmoins convaincus que la plateforme est l'alternative la plus viable à Telegram.

Riot.im

Riot.im (renommé Element en juillet 2020) est une application chat décentralisée basée sur le réseau Matrix[65]. Elle fournit des communications sous forme de conversations individuelles et de groupes, offre certaines fonctionnalités de partage de fichiers et donne aux utilisateurs un choix concernant le contrôle de l'accès à leurs communications[66]. Initialement conçue comme une plateforme collaborative destinée au milieu professionnel, elle ressemble à toutes les autres applications de messagerie instantanée de cette catégorie (p. ex., Slack, Twist, Microsoft Teams)[67]. Pendant leur période de test de plateformes web décentralisées, les partisans de l'EI ont commencé à créer des groupes sur cette plateforme en septembre 2017, suivis peu après par les sympathisants d'al-Qaïda et d'autres groupes djihadistes[68]. Ces groupes maintiennent leur présence sur la plateforme depuis 2017[69]. Toutefois, la plupart d'entre eux ayant choisi de stocker les communications sur le serveur public de l'entreprise, les réseaux djihadistes présents sur les serveurs de Riot.im connaissent des perturbations régulières dues à des efforts de suppression de contenus et de clôture de comptes[70]. Les observateurs des groupes d'extrême droite en ligne ont également remarqué que certaines des principales chaînes d'extrême droite sur Telegram commencent à s'établir sur Riot.im[71].

Riot.im étant fondée sur la plateforme décentralisée Matrix, les observateurs des activités extrémistes en ligne s'inquiétaient que l'application « devienne une version améliorée de Telegram » si les extrémistes décidaient d'y installer leurs propres serveurs[72]. L'application donne le choix aux utilisateurs de stocker leurs communications sur le serveur public de matrix.org, sur un serveur premium payant hébergé par l'utilisateur lui-même (ou son organisation), sur d'autres serveurs publics créés par des utilisateurs de Riot.im ou sur des serveurs personnalisés[73]. Ainsi, si la plateforme propose des serveurs décentralisés, l'utilisateur doit toutefois s'inscrire puis gérer le serveur. Que les communications soient stockées sur un serveur centralisé et public ou sur un serveur

63 @HoopMessenger, 2019. « Nous continuerons de fermer les groupes reliés à l'EI. Nous encourageons tous nos utilisateurs à nous informer de la présence de chaînes suspectes par e-mail. Notre équipe étant assez réduite, nous comptons sur le public pour nous aider. N'hésitez pas à contacter notre équipe par e-mail ou message privé si vous avez des questions. » 5 décembre 2019. https://twitter.com/HoopMessenger/status/1202698188160811008.
64 MEMRI, « Pro-ISIS Media Foundation Warns ISIS Supporters Against Using Hoop Messenger ».
65 « Fonctionnalités ». n.d. Riot.im. Consulté le 1er avril 2020. https://about.riot.im/features.
66 *Ibid.*
67 *Ibid.*
68 Flashpoint, « Jihadists Presence Online Decentralizes After Telegram Ban » ; Gluck, « Islamic State Adjusts Strategy to Remain on Telegram ».
69 *Ibid.*
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 avec Jon Lewis, Program on Extremism, 1er avril 2020.
72 Bodó, Loránd. 2018. « Decentralised Terrorism: The Next Big Step for the so-Called Islamic State (IS)? ». VOX – Pol. 12 décembre 2018. https://www.voxpol.eu/decentralised-terrorism-the-next-big-step-for-the-so-called-islamic-state-is/.
73 Riot.im, « Fonctionnalités ».

décentralisé, les utilisateurs peuvent activer le chiffrement de bout en bout pour leurs communications sur Riot.im[74].

Pour créer un compte Riot.im, les utilisateurs devront se doter d'un nom d'utilisateur et d'un mot de passe, et peuvent choisir de fournir une adresse e-mail[75]. Après avoir créé un compte, le propriétaire d'une conversation peut changer ses paramètres, de façon à ce que seuls des utilisateurs triés sur le volet puissent y participer, que seuls les utilisateurs possédant un lien URL vers la conversation puissent y accéder, ou que la conversation soit rendue publique[76]. Les participants peuvent également activer le chiffrement de bout en bout de leurs messages.

Riot.im est basé sur la plateforme Matrix et ses serveurs publics y sont hébergés. Ces deux services sont basés au Royaume-Uni[77]. Les rapports entre Riot.im et Matrix ont des implications notables sur la façon dont les extrémistes perçoivent la confidentialité et la sécurité sur la plateforme. Tout d'abord, les utilisateurs extrémistes de Riot.im choisissent souvent d'héberger leurs communications sur les serveurs publics par défaut de Matrix, plutôt que de créer et de gérer leurs propres serveurs décentralisés[78]. Cela signifie que leurs communications sont régies par les conditions d'utilisation de Matrix et sujettes à des réglementations strictes sur les contenus extrémistes en ligne au Royaume-Uni. Les conditions d'utilisation de Matrix interdisent l'utilisation du service « à des fins illicites ou pour appuyer des activités illégales au regard de la loi britannique/de l'UE », y compris la publication de contenu à caractère terroriste[79]. L'entreprise supprime donc régulièrement des contenus et comptes extrémistes de ses plateformes. Lorsque les groupes extrémistes hébergent du contenu sur des serveurs tiers décentralisés, ils sont souvent confrontés à des coupures et à des efforts indépendants de suppression de la part des propriétaires des plateformes[80]. À l'heure actuelle, peu d'extrémistes ont pris l'initiative d'héberger des conversations Riot.im sur des serveurs autogérés[81].

Rocket.Chat

Rocket.Chat est une plateforme de messagerie instantanée décentralisée qui offre à ses utilisateurs la possibilité d'héberger du contenu et des communications sur leurs propres serveurs et de stocker des supports sur le serveur public Rocket.Chat[82]. Il convient de remarquer qu'en décembre 2018, le média central de l'EI a tenté de gérer son propre serveur sur Rocket.Chat, ce qui constitue l'une des premières tentatives des djihadistes de profiter pleinement des plateformes web décentralisées[83]. L'agence Nashir News Agency de l'EI a hébergé plusieurs chaînes Rocket.Chat sur un serveur appelé Techhaven, dont le guide de l'utilisateur indique qu'il était conçu pour fournir « un forum de discussion ouvert, ainsi qu'une confidentialité

74 *Ibid.*
75 *Ibid.*
76 *Ibid.*
77 « Politique de confidentialité ». n.d. Riot.im. Consulté le 1er avril 2020. https://riot.im/privacy.
78 King. « Islamic State Group's Experiments with the Decentralized Web ».
79 Riot.im, « Politique de confidentialité ».
80 King. « Islamic State Group's Experiments with the Decentralized Web ».
81 *Ibid.* ; Bodó, « Decentralized Terrorism ».
82 « Rocket.Chat ». n.d. Rocket.Chat. Consulté le 1er avril 2020. https://rocket.chat/.
83 BBC News. 2019. « Europol Disrupts IS Propaganda Machine ». 25 novembre 2019, sec. Moyen-Orient. https://www.bbc.com/news/world-middle-east-50545816.

et des innovations numériques aux utilisateurs opprimés situés dans les zones de conflits et ciblés, pour leurs croyances par les régimes autoritaires de l'Occident »a[84]. Depuis, l'EI et d'autres groupes djihadistes, y compris al-Qaïda, ont créé des chaînes et des groupes sur Rocket.Chat[85].

Par rapport aux autres plateformes examinées dans ce rapport, Rocket.Chat ressemble le plus à Riot.im, puisqu'il s'agit de plateformes de messagerie conçues à l'origine à des fins de collaboration professionnelle offrant aux utilisateurs le choix entre des serveurs administrés à l'échelle centrale et des serveurs décentralisés gérés par les utilisateurs eux-mêmes[86]. Il est plus facile de créer et de gérer un serveur sur Rocket.Chat que sur Riot.im. La création d'un compte sur le serveur public Rocket.Chat ou l'inscription à un serveur géré de façon privée nécessitent un nom d'utilisateur, un mot de passe et une adresse e-mail[87]. Une fois le compte créé, les utilisateurs peuvent directement communiquer avec d'autres utilisateurs ou créer des chaînes publiques ou privées sur invitation. La plateforme propose également plusieurs autres fonctionnalités uniques potentiellement utiles aux groupes extrémistes, telles que la traduction automatisée des publications en différentes langues[88].

La possibilité d'héberger des serveurs décentralisés est problématique pour les groupes extrémistes. S'ils choisissent d'héberger leurs communications Rocket.Chat sur le serveur central de l'entreprise, celle-ci peut supprimer les chaînes qui favorisent l'extrémisme conformément à son code de conduite des utilisateurs ou, si les circonstances l'exigent, « est tenue de divulguer vos données personnelles si la loi l'exige ou en réponse à une demande valide des autorités publiques »[89]. Choisir d'héberger ses communications sur un serveur décentralisé peut prendre du temps. Cela nécessite une expertise technique et peut poser d'autres problèmes pour les groupes extrémistes[90]. Trois mois après la création de chaînes par l'agence Nashir News Agency sur le serveur Techhaven, l'hébergeur a été ciblé par des attaques de déni de service rendant la plupart de ses chaînes Rocket.Chat inutilisables[91]. Les serveurs créés spécifiquement pour héberger de la propagande extrémiste peuvent être pris pour cible numérique. En cas d'actions de perturbation réussies, les groupes extrémistes présents sur les plateformes décentralisées comme Rocket.Chat peuvent être forcées de passer de serveur en serveur, ce qui limite l'utilité de la plateforme comme base stable de propagande.

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 *Ibid*.
88 *Ibid*.
89 « Politique de confidentialité de Rocket.Chat ». n.d. Rocket.Chat. Consulté le 1er avril 2020. https://rocket.chat/privacy.
90 King. « Islamic State Group's Experiments with the Decentralized Web ».
91 *Ibid*.

TamTam

TamTam est une messagerie instantanée en ligne gérée par le groupe Mail.ru, l'entreprise russe qui détient la plus grosse part de l'Internet russophone et exploite les plateformes populaires de médias sociaux Vkontakte et Odnoklassniki[92]. TamTam est presque identique à Telegram d'un point de vue structurel, notamment sur le plan des fonctionnalités proposées. L'application offre à ses utilisateurs des chats, des chaînes publiques, des chaînes privées et des conversations de groupe[93]. La similarité entre Telegram et TamTam est voulue. TamTam a été créée comme une alternative à Telegram par le groupe Mail.ru lorsque le gouvernement russe tentait de bloquer les adresses IP Telegram de l'Internet russe[94]. Le groupe Mail.ru entretient des liens étroits avec le gouvernement russe et serait plus enclin que son homologue à répondre aux demandes des forces de l'ordre russe portant sur les informations des utilisateurs[95].

Les partisans de l'EI ont créé un nombre considérable de chaînes et de groupes sur TamTam après l'action coordonnée d'Europol menée en décembre 2019 à l'encontre de Telegram[96]. TamTam a rapidement réagi contre l'accélération des contenus liés à l'EI[97]. Un porte-parole de l'entreprise a indiqué à Vice News que TamTam « s'opposait fortement à la présence de contenus quels qu'ils soient créés par des organisations terroristes sur sa plateforme » et a appelé les utilisateurs à signaler les contenus et les comptes promouvant les groupes terroristes[98]. Après la purge de TamTam, les groupes djihadistes ont commencé à mettre leurs abonnés en garde contre l'utilisation de la plateforme[99]. Par exemple, en février 2020, un groupe de partisans anglophones de l'EI s'appelant « Lions of Tawheed » ont posté sur Rocket.Chat que « le gouvernement russe a accès à tous les comptes TamTam (…) Protégez-vous en supprimant TamTam de votre téléphone ou de votre ordinateur. Utilisez des applications sûres comme Riot, Rocket.Chat et Telegram »[100].

TamTam demande aux utilisateurs de suivre les mêmes procédures que Telegram pour créer un compte et accéder à du contenu. L'application offre le même ensemble de fonctionnalités que Telegram, y compris la possibilité de créer des conversations individuelles, des chaînes à distribution multiple et des conversations en groupes élargis[101]. Les utilisateurs peuvent rendre leurs conversations et chaînes accessibles publiquement ou de façon privée par invitation[102]. Les similarités entre TamTam et Telegram s'étendent même à son nom de domaine : les hyperliens raccourcis de Telegram sont accessibles

92 « Some Messenger Called 'TamTam' Is Trying to Replace Telegram in Russia. What the Heck Is It? » 2018. Meduza. 17 avril 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 *Ibid.*
94 *Ibid.*
95 *Ibid.*
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 *Ibid.*
98 Gilbert, David. 2019. « The Russian Social Network Letting ISIS Back Online ». Vice. 3 décembre 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 mars 2020. https://www.memri.org/cjlab/pro-isis-outlet-lists-safe-messaging-apps-advises-against-using-chinese-russian-apps.
100 *Ibid.*
101 « À propos de TamTam ». n.d. TamTam. Consulté le 1er avril 2020. https://about.tamtam.chat/en/index.html.
102 *Ibid.*

via le nom de domaine t.me, tandis que TamTam utilise tt.me[103]. L'entreprise promeut activement sa compatibilité avec Telegram sur le marché russe en annonçant ouvertement ses similitudes avec Telegram sur les chaînes russes populaires de cette dernière[104].

La grande différence entre Telegram et TamTam réside dans les domaines de la confidentialité et de la sécurité. TamTam est enregistrée en Russie et sa politique relative aux données est « conforme aux lois de la Fédération de Russie »[105]. Cela signifie que TamTam, contrairement à Telegram, adhère activement aux lois russes exigeant des prestataires de services qu'ils fournissent un accès dissimulé (backdoor) au Service fédéral de sécurité (FSB), le principal organisme d'application des lois dans la Fédération de Russie[106]. Si l'application prétend offrir du chiffrement, les experts estiment toutefois qu'elle a potentiellement fourni des copies des clés de chiffrement de TamTam au FSB[107]. L'accord de licence de TamTam interdit explicitement aux utilisateurs de « [véhiculer] l'extrémisme, le terrorisme, de susciter des hostilités fondées sur l'identité raciale, ethnique ou nationale » ou de publier des « informations de nature extrémiste »[108]. Il est raisonnable de supposer que si les partisans de l'EI ont tenté d'exploiter TamTam après les journées d'action de signalement d'Europol en 2019, c'est en raison de ses similitudes avec Telegram plutôt que pour ses fonctionnalités en matière de sécurité et de confidentialité.

103 Meduza, « Some Messenger Called 'TamTam' Is Trying to Replace Telegram in Russia ».
104 *Ibid*.
105 « Politique de confidentialité de TamTam Messenger ». n.d. TamTam. Consulté le 1er avril 2020. https://about.tamtam.chat/en/policy/index.html.
106 *Ibid*.
107 *Ibid*.
108 « Contrat de licence de l'utilisateur final de TamTam Messenger ». n.d. TamTam. Consulté le 1er avril 2020. https://about.tamtam.chat/en/license/index.html.

Figure 1 : Comparaison des plateformes de messagerie instantanée utilisées par les groupes extrémistes

Plateforme	Utilisation par les groupes extrémistes	Pays d'enregistrement	Ensemble de fonctionnalités	Sécurité	Environnement politique/réglementaire
Telegram	Djihadistes (EI, al-Qaïda), extrême droite	Îles Vierges britanniques/ Émirats arabes unis	• Conversations individuelles • Conversations de groupe • Conversations publiques et privées	• Chiffrement de bout en bout pour les conversations individuelles • Auto-destruction du compte/des données	• Supprimera les contenus publics « à caractère terroriste » (bots et chaînes publiques) • Sur ordre d'une juridiction, fournira les informations des utilisateurs aux forces de l'ordre dans les affaires de terrorisme
BCM*	Djihadistes (EI)	Îles Vierges britanniques	• Conversations individuelles • Conversations de groupe	• Chiffrement de bout en bout • Auto-destruction du compte/des données • Possibilité de serveur décentralisé	• Pas de politique connue en matière de suppression ou de modération des contenus à caractère extrémiste • Pas de communication des données des utilisateurs aux forces de l'ordre
Gab Chat**	Extrême droite	États-Unis	• Conversations individuelles • Conversations de groupe	• Chiffrement de bout en bout sur l'appareil • Suppression des messages sur le serveur après 30 jours	• Les discours « choquants » et « haineux » ne sont pas un motif de suppression de contenu ; seuls le sont les « contenus et activités illicites » • Coopérera avec le gouvernement américain uniquement (aucun autre gouvernement ou tiers) lorsque recevra des demandes licites de communication de données des utilisateurs dans le cadre d'une enquête
Hoop Messenger	Djihadistes (EI, al-Qaïda)	Canada	• Conversations individuelles • Conversations de groupe • Chaînes publiques et privées	• Chiffrement de bout en bout sur toutes les conversations et fichiers situés dans un « Coffre-fort » protégé par mot de passe • Suppression à distance des comptes et du contenu du Coffre-fort	• L'entreprise « supprimera les contenus qu'elle considérera, à sa seule discrétion, illicites, obscènes, choquants, menaçants, diffamatoires, insultants ou autrement répréhensibles »

Plateforme	Utilisation par les groupes extrémistes	Pays d'enregistrement	Ensemble de fonctionnalités	Sécurité	Environnement politique/réglementaire
Riot.im	Djihadistes (EI, al-Qaïda), extrême droite	Royaume-Uni	• Conversations individuelles • Conversations de groupe	• Chiffrement de bout en bout activé par l'utilisateur • Possibilité de serveur décentralisé	• L'entreprise peut supprimer le contenu des serveurs publics visant « un quelconque but illicite ou appuyant des activités illégales en vertu du droit britannique/de l'UE »
Rocket.Chat	Djihadistes (EI, al-Qaïda)	États-Unis/Brésil	• Conversations individuelles • Conversations de groupe • Chaînes publiques et privées	• Chiffrement de bout en bout activé par l'utilisateur • Possibilité de serveur décentralisé	• L'entreprise est « tenue de communiquer vos données personnelles si la loi l'exige ou en réponse à des demandes valides des autorités publiques »
TamTam	Djihadistes (EI, al-Qaïda)	Fédération de Russie	• Conversations individuelles • Conversations de groupe • Chaînes publiques et privées	• « Chiffrement » (protocole incertain)	• L'entreprise interdit de véhiculer « l'extrémisme, le terrorisme, de susciter des hostilités fondées sur l'identité raciale, ethnique ou nationale » ou de publier des « informations de nature extrémiste » • « Les données des utilisateurs seront traitées en vertu des lois de la Fédération de Russie », ce qui implique une communication obligatoire des informations et des clés de chiffrement aux forces de l'ordre russes

* Service interrompu, février 2020
** Actuellement en version beta

4 Analyse : la courbe d'adoption des applications de messagerie instantanée par les groupes extrémistes

L'expérimentation des services de messagerie instantanée en ligne menée par les extrémistes constitue une facette importante des efforts qu'ils entreprennent pour adopter des technologies émergentes. Compte tenu des difficultés rencontrées sur Telegram, l'adoption d'applications de messagerie secondaires par les extrémistes suit généralement ce que Daveed Gartenstein-Ross, Matt Shear et David Jones nomment la « courbe d'adoption des technologies par les acteurs non étatiques violents »[109]. Lors des premières phases d'adoption, les extrémistes tentent (généralement sans succès) d'exploiter les technologies émergentes[110]. Pendant la phase d'itération, ils améliorent peu à peu leur capacité à utiliser ces technologies, leur démarche étant favorisée par l'apparition de nouveaux produits sur le marché[111]. Après l'itération, les groupes extrémistes sont susceptibles de connaître une percée – en découvrant une méthode particulière d'utilisation desdites technologies permettant d'asseoir considérablement leurs stratégies[112]. Ils devront toutefois inévitablement affronter la concurrence que représentent les réactions des pouvoirs publics et des prestataires de services[113]. Une concurrence importante peut entraîner un redémarrage de la courbe d'adoption, portant cette fois sur des produits se substituant à la technologie d'origine, les groupes extrémistes étant forcés de tester de nouvelles technologies[114].

La percée réalisée par les extrémistes entre 2015 et 2017 sur Telegram est vraisemblablement en cours de transition vers cette phase de concurrence. Cette dernière année, Telegram, en collaboration avec des agences gouvernementales, a commencé à remettre largement en cause l'usage de la plateforme par les groupes extrémistes, ce qui a poussé les extrémistes de différents bords à revenir à l'étape d'adoption de plusieurs alternatives à Telegram[115]. En utilisant la courbe d'adoption des technologies par les acteurs non étatiques violents comme guide, nous pouvons estimer que la majorité des efforts déployés par les groupes extrémistes pour trouver une alternative durable et sûre à Telegram ont échoué. Pourtant, les capacités d'apprentissage organisationnel rapide des groupes extrémistes relatives à l'adoption de nouvelles plateformes

109 Gartenstein-Ross, Daveed, Matt Shear et David Jones. 2019. « Virtual Plotters. Drones. Weaponized AI?: Violent Non-State Actors as Deadly Early Adopters ». Washington, D.C. : Valens Global. https://valensglobal.com/virtual-plotters-drones-weaponized-ai-violent-non-state-actors-as-deadly-early-adopters/.
110 *Ibid.*
111 *Ibid.*
112 *Ibid.*
113 *Ibid.*
114 *Ibid.*
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 ».

de réseaux sociaux sont incontestables[116]. Avec l'apparition de messageries instantanées de plus en plus stables offrant de nouvelles fonctionnalités en matière de confidentialité et de sécurité, il est plus question de savoir « quand » les extrémistes passeront de Telegram à une messagerie instantanée secondaire, et « laquelle » ils choisiront, plutôt que de savoir « si » ils le feront.

Les groupes extrémistes de différents bords sont susceptibles de quitter Telegram à des périodes différentes, puisqu'ils sont confrontés à une concurrence disparate sur la plateforme. Les mesures prises par l'entreprise et les pouvoirs publics contre les groupes extrémistes sur Telegram, allant de la suppression de contenus et de comptes à des activités de surveillance, se concentrent aujourd'hui sur les partisans de l'EI[117]. Les sympathisants des autres groupes extrémistes, y compris l'extrême droite et d'autres groupes djihadistes, font face à une contestation limitée et sont donc moins enclins à quitter la plateforme[118]. C'est pourquoi les partisans de l'EI sont susceptibles de poursuivre leurs efforts d'expérimentation de nouvelles plateformes de messagerie instantanée pour trouver une solution de rechange à Telegram. Toutefois, si l'application commence à prendre des mesures de répression massives à l'encontre d'autres types d'activités extrémistes menées sur sa plateforme, un plus grand nombre de groupes djihadistes et d'extrême droite pourraient leur emboîter le pas.

Une première analyse des plateformes recensées plus haut peut mettre en lumière certaines des fonctionnalités que les groupes extrémistes recherchent lorsqu'ils adoptent des alternatives à Telegram. L'ensemble d'applications de messagerie instantanée que les groupes extrémistes ont adopté suite à la hausse de la concurrence menée sur Telegram présentent des points communs et tendances notables. Tout d'abord, bon nombre d'entre elles offrent des options et présentations visuelles similaires à celles de Telegram. Ce n'est pas un hasard si TamTam est l'une des premières plateformes à avoir été prises d'assaut par les sympathisants de l'EI au lendemain des journées d'action de signalement d'Europol[119]. Cette application est presque une copie conforme de Telegram, et se décrit même comme tel. Malgré de faibles fonctionnalités en matière de sécurité et de confidentialité, elle a aussitôt attiré les utilisateurs extrémistes de Telegram en raison de sa ressemblance avec cette dernière. Dès le début de la recherche d'une solution de rechange à Telegram, les points communs avec cette dernière ont été considérés comme un avantage par les groupes extrémistes, leurs partisans pouvant ainsi s'adapter rapidement à la nouvelle plateforme, celle-ci assurant ainsi une certaine facilité d'utilisation et familiarité.

L'analyse ci-dessus montre également que les groupes extrémistes testent de plus en plus de plateformes de messagerie instantanée proposant des serveurs et un stockage des données décentralisés.

116 Shapiro, Jacob N. 2015. The Terrorist's Dilemma: Managing Violent Covert Organizations. Réimpression. 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 et 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 et Logan Macnair. 2019. « Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends ». La Haye, Pays-Bas : Centre international de lutte contre le terrorisme. https://icct.nl/wp-content/uploads/2019/11/Right-Wing-Extremists-Persistent-Online-Presence.pdf.

118 Amarasingam, « Telegram Deplatforming ISIS Has Given Them Something to Fight For ».

119 King, « Islamic State Group's Experiments with the Decentralized Web » ; Bodó, « Decentralized Terrorism ».

Jusqu'ici, la plupart d'entre eux semblaient n'avoir pas pleinement profité de la possibilité de décentraliser le stockage de données tout en utilisant des plateformes telles que BCM, Riot.im ou Rocket.Chat[120]. La gestion de serveurs indépendants pour ces plateformes peut être chronophage, demander beaucoup de ressources et, comme l'a découvert l'agence Nashir News Agency lorsqu'elle a tenté de créer un serveur décentralisé Rocket.Chat pour ses chaînes de propagande, créer des cibles supplémentaires pour les gouvernements, la concurrence et les pirates indépendants[121]. Les premières versions de ces plateformes et les efforts rudimentaires déployés par les groupes extrémistes pour les exploiter connaissent nécessairement des complications, dénis de service et autres problèmes de nature technologique. Toutefois, certaines plateformes nouvelles comme ZeroNet et Matrix, entre autres, facilitent l'hébergement de serveurs décentralisés pour les consommateurs, ce qui les rendra inévitablement plus accessibles aux groupes extrémistes[122].

Néanmoins, une plateforme de messagerie instantanée construite sur le web décentralisé peut être une candidate de choix pour remplacer Telegram, en particulier si elle devient facilement accessible pour les extrémistes et est facile à utiliser. Pour Loránd Bodó, « le web décentralisé semble être la suite logique non seulement pour l'EI, mais aussi pour d'autres extrémistes (violents) en ligne tentant d'échapper aux autorités et aux campagnes de suppression »[123]. La motivation pour adopter des plateformes web décentralisées est simple : les extrémistes en ligne sont confrontés à des menaces de la part des gouvernements qui tentent de surveiller, d'identifier et d'interdire l'accès aux terroristes potentiels et des fournisseurs de technologies qui tentent d'éliminer la propagande extrémiste de leurs plateformes[124]. Grâce à Telegram et à d'autres services, les extrémistes sont de plus en plus en mesure d'utiliser les services maximisant la confidentialité, comme le chiffrement de bout en bout, mais se retrouvent face à un combat difficile pour maintenir la résilience de leurs réseaux sur les plateformes[125]. La capacité de ces groupes à stocker des données sur leurs propres serveurs aurait pour conséquence d'atténuer l'effet des efforts de suppression de contenu déployés par les sociétés technologiques en assurant la création d'un réseau de stockage indépendant, décentralisé et hors de la portée des prestataires de services[126].

120 *Ibid.*
121 *Ibid.*
122 *Ibid.*
123 Bodó, « Decentralized Terrorism ».
124 *Ibid.*
125 *Ibid.*
126 *Ibid.*

5 Recommandations : vers une approche de l'extrémisme en ligne fondée sur les fonctionnalités

La prévalence des messageries comparables à Telegram et des applications décentralisées dans les applications chats exploitées par les extrémistes depuis l'arrivée de concurrents sur Telegram montre que l'adoption desdites applications repose sur les fonctionnalités qu'elles proposent. Il appartient par ailleurs aux décideurs chargés de l'élaboration de politiques en matière de lutte contre l'extrémisme en ligne de cesser de prêter attention à certaines plateformes ou applications particulières et de privilégier une approche de l'exploitation par les extrémistes des technologies de communication numérique fondée sur les fonctionnalités. Les chercheurs et décideurs politiques portent leur attention sur un nombre restreint de plateformes « problématiques » – ces dernières années, Twitter et Telegram – et ignorent de ce fait le vaste écosystème de communications extrémistes en ligne[127]. Cette dynamique se traduit par des coups de filet en ligne ciblés tels que les journées d'action de signalement d'Europol, qui ont incité certains décideurs politiques à présenter la suppression de contenus sur certaines plateformes comme des victoires éclatantes contre l'extrémisme en ligne. Comme le prouve ce rapport, l'utilisation décentralisée de plateformes qui en découle peut remettre en cause les effets positifs de ces opérations[128].

Globalement, une approche fondée sur les fonctionnalités bénéficierait à la lutte contre l'extrémisme en ligne, en garantissant la correspondance entre les ripostes politiques et la façon dont les extrémistes se représentent leur utilisation d'Internet. Par ailleurs, en se concentrant sur la lutte contre l'exploitation de certaines fonctionnalités par les extrémistes plutôt que sur leur utilisation de certaines plateformes, les prestataires de services pourront plus aisément trouver des entreprises comparables pour partager leurs réponses et innovations. Les données issues de nombreuses études de plateformes suggèrent que les extrémistes ont privilégié ces applications non en raison de leur nom ou de leur légitimité, mais des fonctionnalités qu'elles proposaient[129].

127 Alexander, Audrey, et Bill Braniff. 2018. « Marginalizing Violent Extremism Online ». Lawfare. 21 janvier 2018. https://www.lawfareblog.com/marginalizing-violent-extremism-online ; Fisher, Ali, Nico Prucha et Emily Winterbotham. 2019. « Mapping the Jihadist Information Ecosystem: Towards the Next Generation of Disruption Capability ». Global Research Network on Terrorism and Technology : Document n° 6, juillet 2020. https://rusi.org/sites/default/files/20190716_grntt_paper_06.pdf.

128 Alexander et Braniff, « Marginalizing Violent Extremism Online ».

129 *Ibid.*

Pour riposter contre l'exploitation d'Internet par les extrémistes, les décideurs politiques européens et américains détenteurs de l'autorité réglementaire ont tendance à cibler certaines plateformes et à exercer des pressions réglementaires sur elles, à leur mettre des bâtons dans les roues et à leur lancer des ultimatums. Dans certains cas, ces mesures peuvent s'avérer nécessaires. Il existe malheureusement des plateformes qui affichent de piètres performances en matière de lutte contre l'extrémisme en ligne en raison d'une application inadéquate de leurs conditions d'utilisation, d'un manque cruel de capacités, d'environnements réglementaires peu propices, voire de partis pris à l'égard de certains groupes extrémistes qui les empêchent d'agir. Il est nécessaire de cibler ces plateformes pour garantir l'application des réglementations en vigueur. Certaines plateformes, attrayantes pour les extrémistes en raison des fonctionnalités qu'elles proposent ou de leur vaste portée, sont toutefois largement exploitées par ces derniers, malgré les efforts déployés en toute bonne foi pour modérer et/ou supprimer des contenus. Une approche fondée sur les fonctionnalités, qui évaluerait l'exploitation par les extrémistes de certaines potentialités proposées, aiderait les décideurs politiques à distinguer les plateformes présentant des problèmes de gouvernance et de modération, qui pourraient répondre positivement aux pressions exercées, de celles qui sont simplement attrayantes pour les extrémistes en raison des fonctionnalités proposées, qui y répondraient moins bien.

Pour les organes chargés de la lutte contre l'extrémisme en ligne tels que le Forum mondial de l'Internet contre le terrorisme (GIFCT), le fait de réunir des plateformes similaires pourrait aider les partenaires à créer des objectifs globaux et holistiques de lutte contre l'extrémisme adaptés aux fonctionnalités communes à plusieurs plateformes. Pour Ali Fisher, Nico Prucha et Emily Winterbotham, « il est essentiel d'axer les efforts sur le paradigme de communication multiplateforme plutôt que sur les plateformes individuelles en vue d'élaborer la prochaine stratégie de déstabilisation en ligne »[130]. Le partage des meilleures pratiques, ripostes et idées entre les plateformes proposant des fonctionnalités similaires, comme les sites de partage de fichiers, les messageries instantanées et les réseaux sociaux, permet d'améliorer la collaboration et l'innovation. Cela peut consolider le partage d'informations existant, comme les bases de données de partage de hash, en permettant à différentes plateformes de retracer la propagation de contenus à caractère extrémiste d'une plateforme à l'autre[131].

Enfin, et surtout, une plus grande collaboration entre les plateformes présentant des fonctionnalités comparables peut servir de système d'alerte précoce concernant le passage des extrémistes d'une plateforme à l'autre. Par exemple, une application de messagerie instantanée membre d'un consortium de partage d'informations formé d'autres plateformes dispose d'une voie directe pour informer ses homologues lorsqu'elle prévoit de prendre des mesures agressives de suppression de contenus et réseaux extrémistes. Les autres plateformes de messagerie instantanée, informées à l'avance que les extrémistes envisageront potentiellement d'utiliser leurs services, peuvent ainsi préparer leur riposte de façon proactive. Le potentiel de déstabilisation par les prestataires de services du processus

130 Fisher *et al.*, « Mapping the Jihadist Information Ecosystem ».
131 *Ibid.*

d'adoption de nouvelles plateformes par les extrémistes dès le stade d'itération pourrait nuire gravement à la création rapide et facile de points de lancement des extrémistes sur de nouvelles plateformes.

À mesure de l'accueil de nouvelles entreprises au sein du GIFCT au cours des prochaines années, celui-ci devra envisager de faire cohabiter ses larges pistes de collaboration actuelles avec des groupes de travail plus restreints réunissant des catégories spécifiques de prestataires. Si ce rapport montre que ce modèle de collaboration peut servir aux plateformes de messagerie instantanée, des recherches et expériences plus approfondies permettraient de déterminer si les autres types de prestataires de services, comme les réseaux sociaux, les systèmes de partage de fichiers ou les plateformes de commerce électronique pourraient bénéficier de groupes spécifiques aux fonctionnalités au sein du Forum. Cette démarche pionnière au sein du GIFCT pourrait également pousser les décideurs politiques et chercheurs à évaluer de façon minutieuse le rôle des fonctionnalités dans l'adaptation extrémiste, ainsi qu'à adapter leurs réponses stratégiques et leurs recherches pour y inclure des pans plus vastes de l'écosystème extrémiste en ligne. En somme, le paradigme spécifique aux fonctionnalités pourrait aider les sociétés technologiques, décideurs politiques, chercheurs et autres professionnels à aplatir la courbe de l'adaptation des technologies de communication numérique par les extrémistes.

Contexte politique

Cette section a été rédigée par Armida van Rij et Lucy Thomas, toutes deux adjointes de recherche au Policy Institute du King's College, à Londres. Elle fournit un aperçu du contexte politique dans lequel s'inscrit ce rapport.

Introduction

L'utilisation, y compris abusive, d'Internet par les terroristes constitue depuis longtemps un défi pour les décideurs politiques, les forces de l'ordre et les sociétés technologiques. Il existe des affaires très publiques d'abus des technologies : la diffusion en direct de l'attentat terroriste en Nouvelle-Zélande en est un exemple flagrant. L'utilisation par les terroristes et les organisations terroristes des applications de messagerie pour planifier leurs activités et trouver de nouvelles recrues constitue toutefois un autre problème potentiel. Les organisations terroristes ont de plus en plus recours aux applications de messagerie chiffrées de bout en bout, précisément parce qu'elles offrent un mode de communication privé, difficilement accessible pour les forces de l'ordre. Ce problème n'a cessé de s'aggraver ces dernières années pour l'application Telegram, mais aussi pour d'autres applications plus récentes, les terroristes cherchant d'autres solutions pour se soustraire à la vue des forces de l'ordre.

Ce rapport présentera certaines des principales difficultés que rencontrent les gouvernements nationaux pour lutter contre l'exploitation des applications de messagerie chiffrées de bout en bout. Il présentera les principales législations en vigueur et les principales parties prenantes dans neuf pays, ainsi que les obstacles rencontrés par les décideurs politiques lorsqu'ils cherchent à empêcher l'utilisation abusive des applications de messagerie, et les problèmes posés par le codage pour les enquêtes des forces de l'ordre. Nous traiterons également des problèmes posés par le passage aux plateformes de messagerie décentralisées et les stratégies éventuelles à mettre en place pour les régir.

Applications de messagerie instantanée et LEV : relever les défis et évaluer les nouvelles avancées

Canada

La stratégie adoptée par le gouvernement canadien en matière de lutte contre le terrorisme et la radicalisation est vaste, et englobe des activités de renseignement et de sécurité traditionnelles, la collaboration avec la société civile, des initiatives collaboratives avec le secteur et la mise en place de services de police axés sur la communauté. Sa stratégie, telle qu'énoncée dans sa Stratégie nationale de lutte contre la radicalisation menant à la violence, comporte trois volets : concevoir des contre-discours en collaboration

avec la société civile, appuyer la recherche relative à la lutte contre l'extrémisme violent (LEV) et développer des partenariats avec des initiatives internationales et des sociétés technologiques[132].

Le Canada a peut-être la stratégie de contre-discours et de collaboration avec la société civile la plus développée de toutes les entités et nations analysées ici. Extreme Dialogue est une initiative de contre-discours mise en place par le gouvernement canadien en collaboration avec l'Institute of Strategic Dialogue. Ce projet fournit des ressources pédagogiques aux professionnels et aux jeunes sous forme de films illustrant les effets négatifs de l'extrémisme[133]. Le Centre canadien d'engagement communautaire et de prévention de la violence est à l'origine d'un certain nombre d'interventions communautaires destinées à lutter contre la radicalisation menant à la violence. À Calgary, par exemple, le programme ReDirect travaille en collaboration avec les services de police municipale et les services communautaires et de voisinage de la ville, ainsi qu'avec des organismes fournissant des services sanitaires et sociaux pour intervenir dès les premiers stades de radicalisation. ReDirect emploie un ensemble de stratégies telles que l'orientation, l'éducation et la fourniture de conseils aux individus cherchant à sortir d'un groupe extrémiste violent[134].

En ce qui concerne l'appui à la recherche en matière de LVE, en 2019, le Canada a confié à Tech Against Terrorism, une initiative internationale parrainée par les Nations Unies travaillant avec le secteur mondial des technologies, la mission de développer une Plateforme d'analyse des contenus à caractère terroriste (TCAP), une base de données qui héberge des supports et contenus terroristes vérifiés provenant de sources libres de droits et d'ensembles de données existants[135]. Cette plateforme peut servir de dispositif d'alerte en direct pour les plateformes en ligne modestes n'ayant pas nécessairement les capacités ou les ressources pour se conformer aux réglementations relatives à la suppression des contenus malveillants et extrémistes.

Enfin, le Canada est partie à un ensemble d'initiatives internationales et transsectorielles. Au lendemain de l'attentat contre la mosquée de Christchuch en mars 2019, le Premier ministre Justin Trudeau s'est joint à l'Appel de Christchurch, un engagement regroupant des États et le secteur des technologies et visant à « supprimer les contenus terroristes et extrémistes violents en ligne »[136]. Outre l'appui à certaines évolutions techniques visant à repérer et supprimer les contenus à caractère extrémistes – tels que la base de données hash du GIFCT – l'appel à l'action incite également les États à appuyer les cadres et activités de renforcement des capacités et de sensibilisation visant à empêcher l'exploitation des services numériques aux fins de diffusion de contenus à caractère terroriste et extrémiste violent[137].

132 « Stratégie nationale de lutte contre la radicalisation menant à la violence »., Sécurité publique Canada. Disponible à l'adresse : https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-strtg-cntrng-rdclztn-vlnc/index-fr.aspx
133 Voir : https://extremedialogue.org/
134 Voir : http://redirect.cpsevents.ca/
135 La TCAP est également mentionnée dans la partie « Contexte politique » du rapport du GNET intitulé « Décrypter la haine : emploi de l'analyse de texte expérimentale aux fins de classification des contenus à caractère terroriste ». Disponible à l'adresse : https://gnet-research.org/wp-content/uploads/2020/09/GNET-Report-Decoding-Hate-Using-Experimental-Text-Analysis-to-Classify-Terrorist-Content_FRENCH.pdf
136 Voir : https://www.appeldechristchurch.com/
137 Voir : https://www.gifct.org/joint-tech-innovation/

Commission européenne

Le Centre européen de lutte contre le terrorisme (ECTC) a été créé au sein d'Europol au lendemain de l'attaque de 2015 visant le personnel du magasine satirique *Charlie Hebdo* à Paris, conformément aux propositions émises dans le Programme européen en matière de sécurité de la Commission européenne. L'ECTC a pour objet d'« améliorer l'échange d'informations et l'appui opérationnel aux enquêteurs des États membres »[138]. La Commission a également lancé le Forum de l'UE sur l'Internet en 2015, qui réunit des États, Europol et des sociétés technologiques et médias sociaux pour garantir la suppression la plus rapide possible des contenus illicites[139].

La Commission européenne reconnaît que les grandes sociétés technologiques ne sont pas les seules à être utilisées et abusées par les organisations terroristes, et que les prestataires de services plus modestes offrant « différents types de services d'hébergement » le sont aussi[140]. Les services de codage sécurisé et les problèmes d'accès aux données privées se sont révélés être des obstacles entravant les enquêtes des forces de l'ordre.

Europol a lancé plusieurs grandes opérations pour éliminer l'EI et ses utilisateurs affiliés de Telegram. En novembre 2019, l'agence a ainsi supprimé 5 055 comptes et bots au total sur plusieurs jours, contre une moyenne journalière de 200 à 300 suppressions de compte à d'autres moments[141]. Selon Telegram, 3 276 comptes ont été supprimés en une seule journée en décembre 2018, et Europol a organisé une autre journée du même type en avril de la même année[142]. Si ces événements pris séparément perturbent considérablement les opérations de l'EI, ils n'auront toutefois probablement pas d'effets durables si les efforts de répression ne sont pas constants.

Parallèlement à ces journées de répression, une collaboration entre Telegram et Europol a également entraîné un renforcement des outils de signalement de contenu, grâce auxquels tout utilisateur peut signaler, en se servant de la fonctionnalité de signalement des groupes et chaînes, du contenu qu'il estime inapproprié[143].

France

En collaboration avec l'Allemagne, la France a appelé la Commission européenne à réglementer les applications de messagerie chiffrées dans le cadre de la lutte antiterroriste[144]. Plus précisément, l'ancien ministre de l'Intérieur français Matthias Fekl a demandé à ce que la police ait un droit d'accès aux services en ligne et technologiques,

138 Commission européenne, Migration et affaires intérieures, *Counter-terrorism and radicalisation*. https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism_en

139 Commission européenne, Service de presse, *Forum de l'UE sur l'internet : réunir les gouvernements, EUROPOL et les entreprises du secteur de l'internet pour lutter contre les contenus à caractère terroriste et les discours de haine en ligne*. 3 décembre 2015. https://ec.europa.eu/commission/presscorner/detail/fr/IP_15_6243

140 Commission européenne, « Proposition de règlement du Parlement européen et du Conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne », COM(2018) 640. 2018/0331. 12 septembre 2018. P. 1 https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52018PC0640&from=EN

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

142 *Ibid*.

143 Europol, « Europol and Telegram Take on Terrorist Propaganda Online ». Communiqué de presse. 25 novembre 2019. https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online

144 Gouvernement français, ministère de l'Intérieur, « Initiative franco-allemande sur la sécurité intérieure en Europe ». 23 août 2016. https://www.interieur.gouv.fr/Archives/Archives-des-actualites/2016-Actualites/Initiative-franco-allemande-sur-la-securite-interieure-en-Europe

comparable à son droit de demander des informations aux entreprises de télécommunication[145].

En réponse à la pression exercée par la France et l'Allemagne, la Commission européenne propose de modifier sa directive sur le respect de la vie privée en ligne, en autorisant les gouvernements nationaux à contourner certaines mesures de protection de la vie privée en cas de menace pour la sécurité nationale – mais cela ne concerne pas le cryptage des données[146]. L'absence de moyens juridiques forçant les sociétés technologiques à communiquer les données codées est un obstacle de taille pour les forces de l'ordre nationales[147]. Depuis la publication des propositions de la Commission européenne en janvier 2017, les négociations à l'échelle du Conseil en sont cependant au point mort et n'ont pas avancé sous la présidence allemande de l'UE[148].

En France à l'heure actuelle, les fournisseurs de chiffrement sont tenus de « signer des accords avec le gouvernement pour faciliter l'accès aux données chiffrées, sous peine d'amende »[149]. En parallèle, Matignon a le pouvoir d'« interdire les services de chiffrement qui ne respectent pas leurs obligations légales »[150].

Ghana

Le nombre d'attentats terroristes ayant touché le Ghana est tellement faible – le pays n'a connu que 21 incidents ayant fait 23 morts depuis 1970[151] – que le gouvernement n'a pas élaboré de cadre de gouvernance solide relatif à l'extrémisme violent en ligne[152].

En revanche, le Nigéria, lui-même situé en Afrique de l'Ouest, se trouve aux prises d'attentats terroristes majeurs depuis plusieurs années. Des groupes comme Boko Haram et l'État islamique en Afrique de l'Ouest ont mené des attentats qui ne sont pas passés inaperçus, comme l'enlèvement d'étudiantes en avril 2014[153] et les massacres de janvier 2015, tous deux perpétrés dans l'État de Borno[154]. Boko Haram a commencé à utiliser les médias sociaux pour diffuser sa propagande et recruter de nouveaux membres. Ce groupe utilise principalement les médias sociaux traditionnels comme Twitter, Facebook et YouTube, pour publier des photos de soldats, annoncer des décapitations et enlèvements et diffuser des messages antigouvernementaux dans le but d'attirer de nouvelles recrues[155]. Ces dernières années toutefois, Boko Haram a commencé à utiliser des applications de messagerie

145 Stupp, C. « L'UE veut faciliter l'accès de la police à WhatsApp ». *Euractiv*. 29 mars 2017. https://www.euractiv.fr/section/soci-t/news/eu-to-propose-new-rules-on-police-access-to-encrypted-data-in-june/
146 *Ibid*.
147 *Ibid*.
148 Parlement européen, *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*. Février 2017, p. 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 *Ibid*.
151 Global Terrorism Database, START. Disponible à l'adresse : https://www.start.umd.edu/gtd/
152 Voir également la section « Contexte politique » du rapport GNET précédent, « Intelligence artificielle et lutte contre l'extrémisme violent : rapport introductif ». Disponible à l'adresse : https://gnet-research.org/wp-content/uploads/2020/09/GNET-Report-Artificial-Intelligence-and-Countering-Violent-Extremism-A-Primer_FRENCH.pdf
153 Mbah, F. (2019), « Nigeria's Chibok schoolgirls: Five years on, 112 still missing », Al Jazeera. Disponible à l'adresse : 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 ». Disponible à l'adresse : https://www.amnesty.org.uk/nigeria-boko-haram-doron-baga-attacks-satellite-images-massacre
155 Programme des Nations Unies pour le développement et RAND. 2018. « Social Media in Africa ». Disponible à l'adresse : https://www.africa.undp.org/content/rba/en/home/library/reports/social-media-in-africa-.html

instantanée chiffrées comme Telegram pour publier sa propagande et dénoncer d'autres groupes[156]. En 2013, en réponse à la hausse du terrorisme dans le pays, le gouvernement nigérian a intensifié sa législation en matière de lutte antiterroriste et de gouvernance. Outre le renforcement des institutions de l'État chargées de la lutte contre le terrorisme, le gouvernement s'est également octroyé le droit d'arrêter et de poursuivre les individus soupçonnés de terrorisme et de prononcer la peine de mort à l'encontre des personnes reconnues coupables d'avoir commis ou planifié un acte terroriste[157].

En ce qui concerne la régulation de Telegram et des autres applications, le voisin régional du Ghana a opté pour un mode de gouvernance traditionnel, descendant et centré sur l'État. Cette forme de gouvernance met davantage l'accent sur les mesures législatives que sur les initiatives transsectorielles ou l'engagement avec la société civile. Par ailleurs, la gouvernance centrée sur l'État a déjà produit des résultats dangereux et imprévus, tels que le blocage d'Internet par les pouvoirs publics ou l'exploitation des réseaux sociaux par le gouvernement pour éliminer l'opposition politique[158]. Certains gouvernements africains ont exploité l'héritage laissé par des lois coloniales violentes, historiquement utilisées pour violer les libertés citoyennes et « justifier de nombreuses (…) tentatives de requêtes extrajudiciaires adressées au secteur privé »[159].Les médias sociaux et les fournisseurs d'accès à Internet ont dû répondre à des requêtes extrajudiciaires de blocage de la part des gouvernements, suscitant ainsi des inquiétudes sur la censure et la violation de la liberté d'expression[160].

Certains groupes de la société civile et journalistes ont exprimé leur inquiétude concernant l'avenir du Ghana en matière de régulation d'Internet et des médias sociaux[161]. Par exemple, le chef de la police ghanéenne a annoncé la possibilité de bloquer les réseaux sociaux avant les élections de 2016 (ce qui n'a heureusement pas eu lieu)[162]. De plus, les lois généreuses relatives à la liberté d'expression dans le pays laissent la place aux abus dans les espaces numériques, comme les discours haineux et le harcèlement en ligne (des femmes en particulier)[163]. Les appels à une régulation plus stricte des médias sociaux vont donc croissant.

En réponse à ces appels, le Ghana a adopté, en 2019, un projet de loi sur le droit à l'information, qui garantit l'accès aux informations détenues par les institutions publiques[164]. Ce projet de loi signale que le gouvernement ghanéen souhaite faire preuve de transparence et

156 Zenn, J. (2017), « Electronic Jihad in Nigeria: How Boko Haram is Using Social Media ». *Terrorism Monitor*, vol. 15, n° 23. Disponible à l'adresse : https://www.refworld.org/docid/5b728ca2a.html
157 « Nigeria: Extremism & Counter Extremism », Counter-Extremism Project. Disponible à l'adresse : 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. Disponible à l'adresse : 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. Disponible à l'adresse : 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 ». Disponible à l'adresse : 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. Disponible à l'adresse : 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 août 2019. Disponible à l'adresse : https://www.accessnow.org/president-ghana-says-no-internet-shutdown-elections-social-media/
163 Endert, J. (2018), « Digital backlash threatens media freedom in Ghana », DW Akademie. Disponible à l'adresse : 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 mars 2019. Disponible à l'adresse : https://www.graphic.com.gh/news/politics/ghana-news-rti-bill-passed.html

de responsabilité dans sa gestion des droits numériques et trouver un équilibre entre protection des utilisateurs contre les préjudices et protection de leur liberté d'expression. Le gouvernement ghanéen pourrait toutefois élargir sa stratégie de lutte contre l'extrémisme violent pour collaborer avec société civile et les groupes communautaires et préparer une riposte conjointe.

Japon

Les actions antiterroristes menées par le gouvernement japonais sont strictement divisées entre ce qui est perçu comme des activités terroristes à l'étranger et terrorisme intérieur. Cette responsabilité institutionnelle partagée s'accompagne de deux approches de la lutte contre l'extrémisme violent en ligne.

En ce qui concerne les menaces intérieures, comme celles pesant sur les Jeux Olympiques 2021 de Tokyo ou celles représentées par l'extrême droite japonaise, la riposte de l'État est largement coordonnée par les forces de l'ordre. Les activités de subversion communiste datant de la Guerre froide ont influencé la gestion des menaces intérieures par l'empire du Soleil levant : la police préfectorale (supervisée par l'Agence de police nationale) et l'Agence d'investigation de sécurité publique (l'agence japonaise de renseignement) dirigent la collecte de renseignements et les activités antiterroristes sur le territoire[165].

Les activités antiterroristes menées dans le pays sont donc centrées sur des architectures répressives et sécuritaires traditionnelles. Compte tenu des aptitudes nationales aux développements technologiques innovants, le Japon a pris les devants avec la création de solutions d'intelligence artificielle, notamment des systèmes de reconnaissance faciale de grande échelle, d'authentification biométrique et de détection comportementale[166]. Ces solutions suggèrent un modèle de gouvernance axé sur la détection précoce et la prévention, appliqué à l'aide de tactiques répressives et sécuritaires traditionnelles.

Pour consolider ces efforts, le Premier ministre japonais Shinzo Abe a réussi, à la fin du premier semestre 2017, à faire adopter un projet de loi antiterroriste[167] décrit par le chef de l'opposition comme « violent »[168]. Ce projet de loi érige en infraction les préparatifs pour commettre 270 « infractions graves », y compris les sit-ins de protestation et la violation des droits d'auteur d'œuvres musicales,

165 Kotani, K., « A Reconstruction of Japanese Intelligence: Issues and Prospects », in : Philip H. J. Davies et Kristian C. Gustafson (dir.), *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere* (Washington D.C. : Georgetown University Press, 2013), p. 181–99.

166 Gouvernement du Japon. « All is Ready for a Safe and Secure Tokyo Games ». Automne/hiver 2019. Disponible à l'adresse : 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. Disponible à l'adresse : https://www.nec.com/en/press/201502/global_20150219_01.html ; Kyodo News, « Kanagawa police eye AI-assisted predictive policing before Olympics », 29 janvier 2018. Disponible à l'adresse : https://english.kyodonews.net/news/2018/01/5890d824baaf-kanagawa-police-eye-ai-assisted-predictive-policing-before-olympics.html

167 Le projet de loi a été adopté « de façon inhabituelle, sans être soumis au vote de la Commission des affaires judiciaires de la Chambre haute ». Fédération des barreaux du Japon, « 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 juin 2017. Disponible à l'adresse : 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 juin 2017. Disponible à l'adresse : https://foreignpolicy.com/2017/06/16/japan-just-passed-a-brutal-defective-anti-terror-law/

et son application s'étend aux médias sociaux[169]. Les défenseurs des droits de l'homme et groupes de la société civile sont vivement préoccupés par ce texte, compte tenu de son champ d'application large et des vastes pouvoirs de répression et de surveillance des activités en ligne qu'il octroie[170].

En ce qui concerne la lutte contre le terrorisme international, l'approche adoptée par le Japon se distingue de sa stratégie de criminalisation mise en œuvre à l'échelle nationale. Ces efforts sont régionaux, coopératifs et fondés sur le renforcement des capacités. Plus précisément, bon nombre d'entre eux s'inscrivent dans le cadre des activités de l'Association des nations de l'Asie du Sud-Est (ANASE)[171], qui a émis un ensemble de déclarations engageant les signataires à « prévenir, empêcher et combattre le terrorisme international grâce à l'échange d'informations, le partage de renseignements et le renforcement des capacités », et établissant ainsi un précédent en matière de coopération régionale pour la lutte contre l'extrémisme violent et le terrorisme[172].

Le Japon a accueilli à deux reprises le Dialogue ANASE-Japon sur la lutte contre le terrorisme, et dirigé des discussions bilatérales avec différents acteurs mondiaux[173]. Fin 2019, le Japon et le Royaume-Uni ont échangé sur « la situation actuelle en matière de terrorisme international, les mesures à prendre à l'échelle nationale pour lutter contre le terrorisme, ainsi que la coopération actuelle en vue du renforcement des capacités de lutte antiterroriste, en particulier dans les pays tiers »[174].

La lutte contre l'utilisation de Telegram et d'autres applications par les extrémistes au Japon est susceptible de suivre cette double approche : une stratégie orientée vers l'extérieur de coopération et de définition de programmes régionaux, avec une mise en œuvre nationale fondée sur des activités répressives, sécuritaires et de surveillance traditionnelles.

Nouvelle-Zélande

Dévoilée en février 2020, la stratégie antiterroriste générale de la Nouvelle-Zélande montre que la lutte contre l'extrémisme violent en ligne est dirigée par de nombreux organismes et agences qui travaillent en collaboration[175]. À l'instar du Canada (susmentionné), ces organes vont du Comité du Cabinet chargé des relations

169 McCurry, J., « Japan passes "brutal" counter-terror law despite fears over civil liberties », *The Guardian*, 15 juin 2017. Disponible à l'adresse : 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 juin 2017. Disponible à l'adresse : http://www.thedailybeast.com/japans-terrible-anti-terror-law-just-made-the-minority-report-reality

170 Fédération des barreaux du Japon, « 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 juin 2017. Disponible à l'adresse : https://www.nichibenren.or.jp/en/document/statements/170615.html

171 « Japan: Extremism & Counter Extremism », Counter-Extremism Project. Disponible à l'adresse : https://www.counterextremism.com/countries/japan

172 « ASEAN-Japan Joint Declaration for Cooperation to Combat International Terrorism », ANASE. Disponible à l'adresse : https://asean.org/?static_post=asean-japan-joint-declaration-for-cooperation-to-combat-international-terrorism-2

173 « Japan: Extremism & Counter Extremism », Counter-Extremism Project. Disponible à l'adresse : https://www.counterextremism.com/countries/japan

174 Ministère des Affaires étrangères du Japon, « The 4th Japan-the UK Counter-Terrorism Dialogue », 4 décembre 2019. Disponible à l'adresse : https://www.mofa.go.jp/fp/is_sc/page1e_000297.html

175 Gouvernement de Nouvelle-Zélande, Comité des fonctionnaires chargés de coordonner la sécurité intérieure et extérieure, Comité de coordination de la lutte contre le terrorisme, « Countering terrorism and violent extremism national strategy overview », février 2020. https://dpmc.govt.nz/sites/default/files/2020-02/2019-20 CT Strategy-all-final.pdf

extérieures et de la sécurité aux agences de communication des services de police, de renseignement et de sécurité, en passant par les organismes chargés des affaires étrangères, du commerce, de la défense, du transport, de l'innovation et du développement.

Le leadership dont à fait preuve la Nouvelle-Zélande dans différentes initiatives transfrontalières et transsectorielles a retenu l'attention de la communauté internationale. En particulier, après la fusillade de la mosquée de Christchurch en mars 2019, les gouvernements de la Nouvelle-Zélande et de la France ont formé une coalition de chefs d'État et de sociétés technologiques et de médias sociaux dans le cadre de l'Appel de Christchurch pour supprimer les contenus terroristes et extrémistes violents en ligne[176]. Les États signataires s'engagent, dans le cadre de cet appel, à assurer l'application des lois interdisant la diffusion de contenus à caractère terroriste et extrémiste violent en ligne tout en respectant les principes de liberté d'expression et de confidentialité. Les pays œuvrent également pour appuyer les cadres et activités de renforcement des capacités et de sensibilisation visant à empêcher l'utilisation des services numériques à des fins de diffusion de contenus à caractère terroriste et extrémiste violent.

L'Appel de Christchurch engage également les sociétés, y compris Amazon, Facebook, Google, Twitter et YouTube, à adopter des normes sectorielles plus strictes en matière de responsabilité et de transparence. Ces sociétés doivent assurer l'exécution de leurs normes communautaires et conditions d'utilisation en accordant la priorité aux mesures de modération et de suppression de contenu et en identifiant les contenus en temps réel pour examen et évaluation. Ensemble, les pays et sociétés déploient des efforts en conjonction avec la société civile pour promouvoir les activités communautaires afin d'intervenir dans les processus de radicalisation en ligne.

L'appel a également servi de support au processus de révision du GIFCT. Dans le cadre de ce processus, le mandat du GIFCT a été élargi pour inclure un ensemble d'activités de prévention, de riposte et d'éducation dans les efforts de lutte contre l'extrémisme violent en ligne[177].

Les efforts menés par la Nouvelle-Zélande pour coparrainer un ensemble d'initiatives mondiales transsectorielles montrent l'approche horizontale adoptée par le pays pour régir l'utilisation des plateformes technologiques par les extrémistes. Cette démarche compte des structures conventionnelles dédiées à la sécurité et au renseignement, ainsi que des initiatives rassemblant des professionnels, des chercheurs, des décideurs politiques et les leaders du secteur des technologies qui unissent leurs forces pour apporter des réponses aux menaces extrémistes violentes apparaissant sur la toile.

Royaume-Uni

La stratégie du Royaume-Uni en matière de lutte contre l'utilisation des plateformes en ligne par les groupes extrémistes suit un mode de gouvernance traditionnel axé sur les institutions de l'État.

176 Voir : https://www.appeldechristchurch.com/
177 Forum mondial de l'Internet contre le terrorisme, « Next Steps for GIFCT », 23 septembre 2019. Disponible à l'adresse : https://gifct.org/press/next-steps-gifct/

L'organisme central responsable de la législation en matière de lutte antiterroriste est le ministère de l'Intérieur (Home Office), qui travaille en coordination avec le quartier-général des communications du gouvernement, l'organisation nationale chargée des questions de sécurité et de renseignement. Le ministère de l'Intérieur a aussi créé des instances de collaboration avec d'autres institutions gouvernementales (généralement le ministère du Numérique, de la Culture, des Médias et des Sports) et le Parlement, tels que le Conseil du Royaume-Uni pour la sécurité d'Internet, l'Office national de sécurité antiterroriste et la Commission de lutte contre l'extrémisme[178].

À l'instar du Japon (ci-dessus), l'approche adoptée par le Royaume-Uni pour lutter contre l'extrémisme violent en ligne comporte deux volets. Le premier volet de ses activités tourne autour de la réglementation des réseaux sociaux et plateformes technologiques. Le Livre blanc du gouvernement sur les dangers en ligne (Online Harms White Paper), publié en avril 2019, a présenté un argumentaire complet pour une meilleure régulation nationale des médias sociaux[179]. En vertu de ce nouveau cadre réglementaire, les sociétés technologiques et médias sociaux auront un nouveau devoir légal de diligence à l'égard de leurs utilisateurs, supervisé par Ofcom, l'organisme britannique de régulation des communications. Ofcom soumettra les plateformes à des sanctions financières et techniques – les sites pourraient être bloqués par les fournisseurs d'accès à Internet et devoir payer une amende s'élevant à 4 % maximum de leur chiffre d'affaires mondial – pour non-respect du cadre et violation du devoir légal de diligence[180]. Au moment de la rédaction de ce rapport, le projet de loi sur les dangers en ligne, la concrétisation législative du Livre blanc, a été retardé de plusieurs années[181].

Le deuxième volet de l'approche du Royaume-Uni tourne autour des services conventionnels de répression, de sécurité et de renseignement, et est consolidé par les lois antiterroristes et un soutien public important. Au printemps 2020, le Parlement a présenté de nouvelles propositions de lois antiterroristes ciblant les individus soupçonnés d'activités terroristes. Dans le cadre de la nouvelle législation, les suspects « qui n'ont pas été reconnus coupables d'une infraction pourraient être soumis à des mesures de surveillance étendues et renforcées »[182]. La durée de ces mesures de surveillance ne serait plus limitée à deux ans. Par ailleurs, il sera désormais plus facile, grâce à une proposition d'allègement de la charge de la preuve, d'imposer des mesures de prévention du terrorisme et d'enquête, telles que la relocalisation forcée, la surveillance et les bracelets électroniques, l'interdiction de fréquenter certains lieux et la limitation des déplacements, des réunions, de l'accès aux services financiers et de l'usage des moyens de communication[183].

178 Gov.uk, « UK Council for Internet Safety ». Disponible à l'adresse : https://www.gov.uk/government/organisations/uk-council-for-internet-safety ; Gov.uk, « Commission for Countering Extremism ». Disponible à l'adresse : https://www.gov.uk/government/organisations/commission-for-countering-extremism ; Gov.uk, « National Counter Terrorism Security Office ». Disponible à l'adresse : https://www.gov.uk/government/organisations/national-counter-terrorism-security-office

179 Gouvernement britannique, « Online harms – White Paper », avril 2019. Disponible à l'adresse : 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 juin 2020. Disponible à l'adresse : https://www.bbc.co.uk/news/technology-53222665

181 *Ibid.*

182 « United Kingdom: Extremism & Counter Extremism », Counter-Extremism Project. Disponible à l'adresse : https://www.counterextremism.com/countries/unitedkingdom

183 Grierson, J., « Unconvicted terrorism suspects face indefinite controls under UK bill », *The Guardian*, 20 mai 2020. Disponible à l'adresse : https://www.theguardian.com/politics/2020/may/20/unconvicted-terrorism-suspects-face-indefinite-controls-under-uk-bill

Ces mesures antiterroristes plus strictes ont été adoptées à la suite des attentats du Fishmongers' Hall, à Londres, en novembre 2019, et de Streatham High Road en février 2020[184], alors que l'opinion publique soutenait le durcissement de la législation[185]. Compte tenu de cette propension permissive, les stratégies de lutte contre l'extrémisme violent en ligne, en particulier l'utilisation d'applications comme Telegram et ses alternatives, pourraient bien abandonner leur nature réglementaire pour endosser un caractère plus répressif. En vertu de la proposition de loi, il suffira d'avoir des « motifs raisonnables » pour soumettre les citoyens à des mesures de prévention du terrorisme et d'enquête[186]. On ignore si le recours à des applications comme Telegram ou d'autres applications de messagerie instantanée décentralisées et chiffrées pour diffuser ou accéder à des contenus à caractère extrémiste relèvera de « motifs raisonnables ».

Direction exécutive du Comité contre le terrorisme des Nations Unies

L'Assemblée générale des Nations Unies a adopté à l'unanimité la Stratégie antiterroriste mondiale des Nations Unies en 2006. Depuis, le Conseil de Sécurité a adopté plusieurs résolutions en matière de lutte contre le terrorisme exhortant les États membres de coopérer pleinement à la lutte antiterroriste. Les résolutions 1373 (2001) et 1566 (2004) « requièrent que des mesures législatives (…) soient prises par tous les États Membres pour combattre le terrorisme, au moyen notamment d'une coopération accrue avec les autres gouvernements »[187]. La résolution 1963 (2010) reconnaît quant à elle l'usage accru d'Internet par les terroristes à des fins terroristes[188].

La lutte contre l'utilisation par les organisations terroristes des plateformes décentralisées pose problème aux autorités responsables du maintien de l'ordre. Ces plateformes ne nécessitent aucun intermédiaire pour envoyer et recevoir des messages, ce qui rend très difficile le repérage des terroristes (présumés)[189].

Les Nations Unies ont exhorté les gouvernements nationaux à donner « un fondement juridique clair aux obligations imposées aux parties du secteur privé », en vertu duquel les sociétés et plateformes technologiques devraient coopérer avec les forces de l'ordre dans le cadre de leurs enquêtes[190].

184 Ministère de la Justice du Royaume-Uni, « Press release: 14-year minimum jail terms for most dangerous terror offenders », 20 mai 2020. Disponible à l'adresse : https://www.gov.uk/government/news/14-year-minimum-jail-terms-for-most-dangerous-terror-offenders

185 Dans un rapport de septembre 2017 comprenant un sondage sur les attitudes vis-à-vis des contenus à caractère extrémiste en ligne, près des trois quarts des personnes interrogées ont indiqué être prêtes à appuyer une nouvelle législation érigeant en infraction la possession et la consommation de contenus à caractère extrémiste en ligne. Voir : Frampton, M. (2017), « The New Netwar: Countering Extremism Online ». *Policy Exchange*. Disponible à l'adresse : 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 », juin 2020. Disponible à l'adresse : https://publications.parliament.uk/pa/cm5801/cmpublic/CounterTerrorism/memo/CTSB07.pdf

187 UNODC. *Utilisation de l'Internet à des fins terroristes*. Nations Unies. 2012, p. 18. Disponible à l'adresse : https://www.unodc.org/documents/terrorism/Publications/The_Use_of_Internet_for_Terrorist_Purposes/Use_of_the_Internet_for_Terrorist_Purposes_French.pdf.

188 *Ibid.*

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

190 UNODC. 2012, p. 147.

États-Unis

L'approche stratégique des États-Unis en matière de lutte contre l'utilisation abusive des plateformes technologiques peut être qualifiée d'irrégulière. En ce qui concerne les organismes étatiques qui se retrouvent en première ligne de la riposte, citons le ministère de l'Intérieur (Department of Homeland Security, DHS), le ministère de la Justice, le Federal Bureau of Investigation (FBI), le Centre national antiterrorisme, le Conseil de sécurité nationale et le Congrès, entre autres[191]. Plusieurs méthodes ont été testées : « contre-discours, notes de sensibilisation, partenariats et législation »[192].

Parmi ces méthodes figure le coparrainage d'initiatives transsectorielles mondiales. La Stratégie de lutte contre le terrorisme des États-Unis s'engage à collaborer avec les entreprises et le secteur pour lutter contre les processus de recrutement, de levée de fonds et de radicalisation terroristes en ligne. En ce qui concerne les initiatives transnationales, les États-Unis travaillent avec des initiatives comme Tech Against Terrorism et le Forum mondial de lutte contre le terrorisme, fondé sur un partenariat avec d'autres signataires, la société civile et le secteur des technologies pour concevoir des approches de lutte contre l'extrémisme violent en ligne à moyen et long terme.

Plus généralement, l'administration Obama a mis sur pied un groupe de travail chargé de la lutte contre l'extrémisme violent (Countering Violent Extremism Task Force) en 2011, dans le but d'« unifier les efforts de LVE sur le territoire »[193]. Ce groupe de travail a pour objet de rassembler des professionnels des organismes susmentionnés pour coordonner la collaboration avec la société civile, élaborer des modèles d'intervention, investir dans la recherche et cultiver des stratégies numériques et de communication[194]. Compte tenu des efforts déployés épisodiquement par le pays dans le passé, une approche unifiée de la lutte contre l'extrémisme violent en ligne permettrait de stimuler les efforts de lutte contre l'utilisation abusive des plateformes comme Telegram.

Toutefois, début 2017, le président Trump a réfléchi à une restructuration du groupe de travail afin de supprimer de son champ d'application les actes de terrorisme perpétrés par les suprémacistes blancs, renommant le programme « Lutte contre l'extrémisme radical islamique » (Countering Radical Islamic Extremism)[195]. Par ailleurs, le budget dévoilé au printemps 2017 a mis fin à tous les financements destinés aux programmes de lutte contre l'extrémisme violent[196]. Dès la fin du mois d'octobre 2018, le groupe de travail n'existait plus : les fonds avaient expiré et « ses membres étaient retournés dans leurs départements et agences d'origine »[197].

---

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, p. 5. Disponible à l'adresse :* https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/A%20Plan%20for%20Preventing%20and%20Countering%20Terrorist%20and%20Violent%20Extremist.pdf

192 *Ibid*.

193 Ministère de l'Intérieur, « Countering Violent Extremism Task Force ». Disponible à l'adresse : https://www.dhs.gov/cve/task-force

194 *Ibid*.

195 Ainsley, J. *et al.*, « Exclusive : Trump to focus counter-extremism program solely on Islam – sources ». *Reuters*, 3 février 2017. Disponible à l'adresse : 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 mai 2017. Disponible à l'adresse : https://www.reuters.com/article/us-usa-budget-extremism-idUSKBN18J2HJ

197 Beinart, P. « Trump Shut Programs to Counter Violent Extremism ». *The Atlantic*, 29 octobre 2018. Disponible à l'adresse : https://www.theatlantic.com/ideas/archive/2018/10/trump-shut-countering-violent-extremism-program/574237/

Les mesures prises par Trump témoignent d'une hostilité profonde vis-à-vis des efforts de LVE généralement, et plus particulièrement envers ceux destinés à assurer la sensibilisation communautaire et l'engagement avec la société civile locale et ceux ciblant le terrorisme d'extrême droite et suprémaciste blanc. Par exemple, l'un des bénéficiaires des fonds du DHS était Life After Hate, une initiative aidant les individus souhaitant quitter les groupes suprémacistes blancs et néonazis[198]. La suppression des financements et l'exclusion de la suprématie blanche du champ d'application des efforts menés par les États-Unis peuvent être vues comme un signal évident que l'administration Trump ne prendra pas de mesures à l'encontre des auteurs d'attentats terroristes racistes et suprémacistes.

Cette tendance a de graves conséquences pour la lutte contre l'utilisation de Telegram et d'autres applications de messagerie instantanée chiffrées et décentralisées. Comme le montre Bennett Clifford dans le présent rapport, bon nombre de ces plateformes sont utilisées par les groupes d'extrême droite pour coordonner leurs activités. Si les réponses gouvernementales à ces plateformes endossent un caractère « politiquement motivé et dangereux »[199], nous pouvons raisonnablement nous inquiéter pour l'avenir de la LVE. La dernière ligne de défense contre l'exploitation de ces plateformes sera la pression accrue exercée sur leurs créateurs pour qu'ils respectent les demandes des forces de l'ordre et des tribunaux, une démarche qui s'avérera sans aucun doute trop insuffisante et tardive.

Vers un mode de gouvernance décentralisé des plateformes décentralisées ?

Dans le présent rapport, Bennett Clifford nous alerte sur la progression des applications comme Telegram vers l'hébergement de serveurs décentralisés. Cette fonctionnalité, qui accompagne l'émergence du web 2.0, permettrait aux utilisateurs de communiquer directement les uns avec les autres en évitant les services centralisés fournis par les entreprises comme Google, Amazon, Microsoft et Facebook[200]. Le modèle décentralisé « inverse la tendance actuelle en matière de propriété des données », de telle façon que les utilisateurs ont le plein accès et la pleine propriété sur leurs propres données[201].

La prestation de services centralisés détenus par l'État offre de nombreuses occasions de commettre des abus et autres actes de surveillance et de censure. Par exemple, le gouvernement indien a imposé la plus longue fermeture d'Internet au monde au Cachemire dans le cadre de dizaines d'années de violences et atrocités commises à l'encontre des musulmans dans le pays[202]. Cette déconnexion, d'une durée de 192 jours, s'inscrit dans le cadre d'une attitude inquiétante plus générale vis-à-vis des droits numériques en Inde :

198 Life After Hate, « About Us ». Disponible à l'adresse : https://www.lifeafterhate.org/about-us-page

199 Southern Poverty Law Center. « Trump's planned changes to government's "Countering Violent Extremism" program are politically motivated, dangerous ». 2 février 2017. Disponible à l'adresse : 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 septembre 2018. Disponible à l'adresse : 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 décembre 2018. Disponible à l'adresse : 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 décembre 2019. Disponible à l'adresse : https://www.opendemocracy.net/en/openindia/india-escalating-kashmir-conflict-painting-it-terrorism/

le ministre des Technologies de l'information et de la communication a remis en question le droit des citoyens à Internet, en annonçant que « si le droit à Internet est important, la sécurité du pays l'est tout autant (…) Pouvons-nous nier que les terroristes abusent d'Internet ? »[203].

De même, il est de notoriété publique que les entreprises abusent des données des utilisateurs. En 2018, l'entreprise de conseil politique Cambridge Analytica a récolté les données personnelles de millions d'utilisateurs de Facebook à des fins de publicité politique[204]. Cette fuite de données, la plus importante de l'histoire de Facebook, a été utilisée en 2016 par le candidat à la présidence américaine Donald Trump pour micro-cibler les utilisateurs de Facebook considérés comme des électeurs versatiles[205]. Les données des utilisateurs étant centralisées sur les serveurs de Facebook, la plateforme peut monétiser, surveiller et abuser des informations sensibles et personnelles de milliards de personnes[206].

Le modèle Internet décentralisé, tout en protégeant les données en les gardant hors d'atteinte, n'est pas sans poser des difficultés lui aussi. Les applications de messagerie instantanée décentralisées et chiffrées, comme Telegram et ses alternatives, peuvent offrir un refuge aux contenus à caractère extrémiste. Comme l'indique Bennett Clifford dans le présent rapport, la fonction d'hébergement de serveurs décentralisés sur les plateformes émergentes « rendra inévitablement ces plateformes plus accessibles aux groupes extrémistes ». Une plateforme décentralisée peut beaucoup plus aisément se soustraire à la surveillance et aux interventions à la fois des plateformes autorégulées et des ordres des autorités responsables du maintien de l'ordre, puisqu'elle ne détient plus les données des utilisateurs.

La lutte contre l'exploitation et l'utilisation abusive des plateformes de messagerie instantanée décentralisées soulève des questions relatives à la gouvernance qu'il est urgent – mais difficile – de résoudre. Comment les gouvernements et entreprises peuvent-ils riposter à l'utilisation par les groupes extrémistes d'un Internet décentralisé ? Comment trouver un équilibre entre les droits des utilisateurs au respect de la vie privée et à la liberté d'expression et l'exploitation des plateformes par les extrémistes pour diffuser de la propagande et de fausses informations, rallier de nouvelles recrues à leur cause et préparer des attentats terroristes ?

Les modes de gouvernance actuels offrent trois trajectoires possibles, chacune largement reliée à une phase d'un processus linéaire de radicalisation.

La première approche – la prévention précoce – vise à intervenir dès les premiers stades de radicalisation pour empêcher les personnes de consommer des contenus à caractère terroriste.

---

203 Shastry, V. « Asia's Internet Shutdowns Threaten the Right to Digital Access ». *Chatham House*, 18 février 2020. Disponible à l'adresse : 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 avril 2018. Disponible à l'adresse : https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

205 Hilder, P. et Lewis, P. « Leaked: Cambridge Analytica's Blueprint for Trump's Victory ». *The Guardian,* 23 mars 2018. Disponible à l'adresse : 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 février 2019. Disponible à l'adresse : https://palladiummag.com/2019/02/14/facebooks-political-problems-are-inherent-to-centralized-social-media/

Pour les applications comparables à Telegram, la prévention précoce veillerait à empêcher les gens de chercher à consommer des contenus ou chaînes à caractère extrémiste ou à nouer le contact avec des groupes extrémistes sur la plateforme. Cette approche a l'avantage de réduire la nécessité d'un contrôle coûteux de la plateforme et d'affaiblir la présence en ligne des extrémistes tout en maintenant les droits à la vie privée et à la liberté d'expression des utilisateurs.

Les programmes de prévention précoce présentent toutefois eux-mêmes d'autres difficultés d'ordre éthique, politique et juridique. Le programme de prévention précoce le plus connu est probablement la stratégie « Prevent » du ministère britannique de l'Intérieur, introduite en 2003. Cette stratégie cible « les individus vulnérables au recrutement », en particulier au sein d'institutions comme le système de santé britannique (NHS), les écoles, les universités et d'autres communautés locales et groupes de la société civile[207]. Cette stratégie a, dès le début, été décriée par les groupes de défense des libertés civiles : Shami Chakrabarti, alors directrice de Liberty, un groupe influent de défense des droits, a qualifié Prevent de « plus grand programme d'espionnage des temps modernes au Royaume-Uni », puisque les renseignements recueillis sur lesdits individus vulnérables portaient sur leurs points de vue politiques et religieux, leur santé mentale et leur activité sexuelle[208]. Prevent cible en grande majorité les citoyens musulmans, consolidant ainsi l'islamophobie et assimilant « une résistance politique légitime chez les jeunes musulmans britanniques » à des « indicateurs d'extrémisme violent »[209].

Le deuxième mode de gouvernance est axé sur le désengagement et la production de contre-discours. Les individus qui ont déjà accès à des contenus extrémistes en ligne et les consomment peuvent être ciblés par des contre-discours visant à proposer « d'autres interprétations crédibles du monde et d'autres perspectives d'action et de libre arbitre que celles transmises par les groupes extrémistes violents » en réaffirmant les valeurs de tolérance, d'ouverture, de liberté et de démocratie[210]. Pour les plateformes de messagerie instantanée comme Telegram, cela pourrait supposer d'infiltrer des chaînes et groupes pour y publier des récits alternatifs dans l'espoir d'éloigner certains individus de la radicalisation.

La publication de contre-discours a du potentiel, mais les communications stratégiques menées par les gouvernements se sont avérées largement inefficaces[211] et ont produit des effets négatifs imprévus. Le programme « Think Again Turn Away » du ministère des Affaires étrangères des États-Unis, dans le cadre duquel des contre-discours ont été diffusés et des querelles ont éclaté sur Twitter avec l'EI et des partisans de l'EI, a provoqué de vives réactions, notamment

207 Ministère britannique de l'Intérieur, « Counter-Terrorism Strategy: The Four Ps: Pursue, Prevent, Protect, Prepare ». Disponible à l'adresse : https://web.archive.org/web/20090711105017/http://security.homeoffice.gov.uk/counter-terrorism-strategy/about-the-strategy1/four-ps/ ; Gouvernement britannique, « CONTEST: The United Kingdom's Strategy for Countering Terrorism », juin 2018. Disponible à l'adresse : 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 octobre 2009. Disponible à l'adresse : 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, n° 3 : p. 396–412.

210 Waldman, S. et Verga, S. (2016), « Countering violent extremism on social media », Centre des sciences pour la sécurité, Recherche et développement pour la défense Canada, p. 7. Disponible à l'adresse : https://cradpdf.drdc-rddc.gc.ca/PDFS/unc262/p805091_A1b.pdf

211 Bartlett, J. et Krasodomski-Jones, A. (2015), « Counter-Speech: examining content that challenges extremism online », *Demos*. Disponible à l'adresse : https://www.demos.co.uk/wp-content/uploads/2015/10/Counter-speech.pdf

de colère[212]. Les recherches dirigées par Demos ont montré que les contre-discours européens publiés sur Facebook suscitaient généralement peu d'engouement[213]. Les initiatives de communication stratégique appuyées par les gouvernements manquent de crédibilité en raison des écarts entre ce qu'ils disent et ce qu'ils font réellement : les messages extrémistes violents sont renforcés par la mise en évidence de l'écart existant entre les valeurs défendues par les gouvernements et leurs actions[214].

Les initiatives de production de contre-discours menées en ligne par la suite ont par conséquent souvent réduit l'implication des gouvernements et été dirigées par le secteur lui-même. Google et sa société mère, Alphabet, ont été les premières à utiliser la « méthode de redirection de contenu », qui cible les individus parcourant les publications en ligne de l'EI et les redirige vers des vidéos YouTube soigneusement choisies contrant les messages prônant l'extrémisme violent[215]. Ces vidéos exposent les individus vulnérables et radicalisés à des discours mettant en lumière des valeurs comme la tolérance, la diversité et l'inclusivité. Le principal partenaire d'Alphabet pour la méthode de redirection des contenus est Moonshot CVE, qui dirige des campagnes de contre-discours dans plus de 28 pays et 15 langues[216]. L'Anti-Defamation League, sise aux États-Unis, s'est alliée à Moonshot CVE pour contrer les activités djihadistes et suprémacistes en ligne[217].

Si les efforts déployés par Moonshot CVE ont le potentiel de perturber le parcours de radicalisation, les solutions mises en place par le secteur pour résoudre des problèmes sociopolitiques profonds présentent leurs propres problématiques. Moonshot CVE, en tant qu'entreprise indépendante, échappe à la surveillance et aux responsabilités incombant aux gouvernements ou à la société civile. Elle ne publie que des données de haut niveau sur ses opérations, et la méthode suivie pour choisir la personne redirigée, de même que les raisons expliquant la redirection, ne sont pas clairement explicitées[218].

Le troisième mode de gouvernance – la régulation des plateformes – intervient vers la fin du processus de radicalisation. Dans le rapport ci-dessus, Bennett Clifford décrit la pression exercée par les forces de l'ordre sur les plateformes telles que Telegram pour faire respecter les ordonnances judiciaires relatives à des activités terroristes présumées. Par exemple, à la page 6, Bennett Clifford décrit les journées d'action de signalement d'Europol qui ont donné naissance à la mise à jour de la politique de confidentialité de Telegram, qui comprend désormais une clause stipulant que la plateforme pourra partager les données des utilisateurs avec les autorités à des fins d'identification en cas de suspicion de contenu extrémiste. D'autres plateformes décrites dans le rapport ci-dessus ont collaboré à différents degrés avec des gouvernements et forces de l'ordre pour lutter contre la prolifération de contenus extrémistes.

212 Katz, R. (2014), « The State Department's Twitter War with ISIS is Embarrassing », *Time*. Disponible à l'adresse : https://time.com/3387065/isis-twitter-war-state-department/
213 Bartlett et 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*. Disponible à l'adresse : https://www.globalcenter.org/wp-content/uploads/2015/09/Does-CVE-Work_2015.pdf, p. 33.
215 Voir : https://redirectmethod.org/
216 Voir : http://moonshotcve.com/work/
217 « ADL and Partners Counter White Supremacists Online Through Google Search ». *Anti-Defamation League*. Disponible à l'adresse : https://www.adl.org/news/press-releases/adl-and-partners-counter-white-supremacists-online-through-google-search
218 Voir : http://moonshotcve.com/work/

Ce mode de gouvernance présente toutefois une difficulté. Les efforts de régulation déployés par les décideurs politiques et forces de l'ordre ressemblent en effet à un jeu du chat et de la souris : une fois qu'une plateforme accepte de collaborer dans le cadre d'une ordonnance judiciaire, une autre prend sa place pour offrir aux utilisateurs des services de protection de la vie privée. Comme le conclut le rapport, « avec l'apparition de messageries instantanées de plus en plus stables offrant de nouvelles fonctionnalités en matière de confidentialité et de sécurité, il est plus question de savoir « quand » les extrémistes passeront de Telegram à une messagerie instantanée secondaire, et « laquelle » ils choisiront, plutôt que de savoir « si » ils le feront ».

Une approche de la lutte contre l'extrémisme en ligne fondée sur les fonctionnalités telle que celle présentée dans les dernières pages du rapport ci-dessus offre la possibilité d'une nouvelle forme de gouvernance dépassant les trois trajectoires décrites plus haut. Chacun des modes présentés ci-dessus s'appuie sur une gouvernance verticale et descendante, souvent assurée par les institutions de l'État et reposant sur une justification législative[219]. La prévention précoce, la production de contre-discours et la régulation relèvent toutes d'une structure de gouvernance « de commande et de contrôle » dans le cadre de laquelle les entités (gouvernements, entreprises, forces de l'ordre, agences de renseignement) élaborent des politiques descendantes.

Un web décentralisé, défini par les fonctionnalités qu'il propose aux utilisateurs, pourrait nécessiter un mode de gouvernance lui-même plus décentralisé. Au lieu d'une structure de gouvernance verticale, une approche horizontale de l'élaboration de politiques imitant la structure d'un Internet décentralisé pourrait s'avérer efficace. Des initiatives transsectorielles, comme l'élargissement du champ d'application du GIFCT tel que décrit par Bennett Clifford à la page 29 du présent rapport, qui réunirait un spectre plus large de prestataires de services et de décideurs politiques et experts universitaires, sont de bons exemples d'approches plus décentralisées.

Dans le précédent rapport, *Intelligence artificielle et lutte contre l'extrémisme violent*, le GNET indiquait qu'un organe réglementaire indépendant serait plus efficace pour modérer les contenus préjudiciables en ligne[220]. Une corégulation entre la société civile, les pouvoirs publics, le secteur technologique et les prestataires de services, supervisée par un organe transnational indépendant, entérinerait un mode de gouvernance de la LVE plus horizontal et inclusif. Cet organe pourrait en effet être axé autour des fonctionnalités des plateformes décentralisées et du contenu extrémiste violent en ligne, comme le suggère Bennett Clifford dans le présent rapport, afin de « préparer [une] riposte de façon proactive (…) [et] déstabilis[er] (…) [le] processus d'adoption de nouvelles plateformes par les extrémistes ». Un tel mode de gouvernance décentralisé pourrait s'avérer très efficace pour s'adapter à l'essor du web décentralisé et en relever les défis.

219 Zwitter, A. et Hazenberg, J. (2020), « Decentralized Network Governance: Blockchain Technology and the Future of Regulation ». *Frontiers in Blockchain*. Disponible à l'adresse : https://www.frontiersin.org/articles/10.3389/fbloc.2020.00012/full

220 GNET. « Intelligence artificielle et lutte contre l'extrémisme violent : rapport introductif », p. 41. Disponible à l'adresse : https://gnet-research.org/wp-content/uploads/2020/09/GNET-Report-Artificial-Intelligence-and-Countering-Violent-Extremism-A-Primer_FRENCH.pdf

Global Network
on Extremism & Technology

COORDONNÉES

Pour toute question, demande d'information et demande de copies supplémentaires du présent rapport, contacter :

ICSR
King's College London
Strand
Londres WC2R 2LS
Royaume-Uni

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter : **@GNET_research**

Ce rapport peut, comme toutes les autres publications du GNET, être téléchargé gratuitement à partir du site Internet du GNET : www.gnet-research.org.