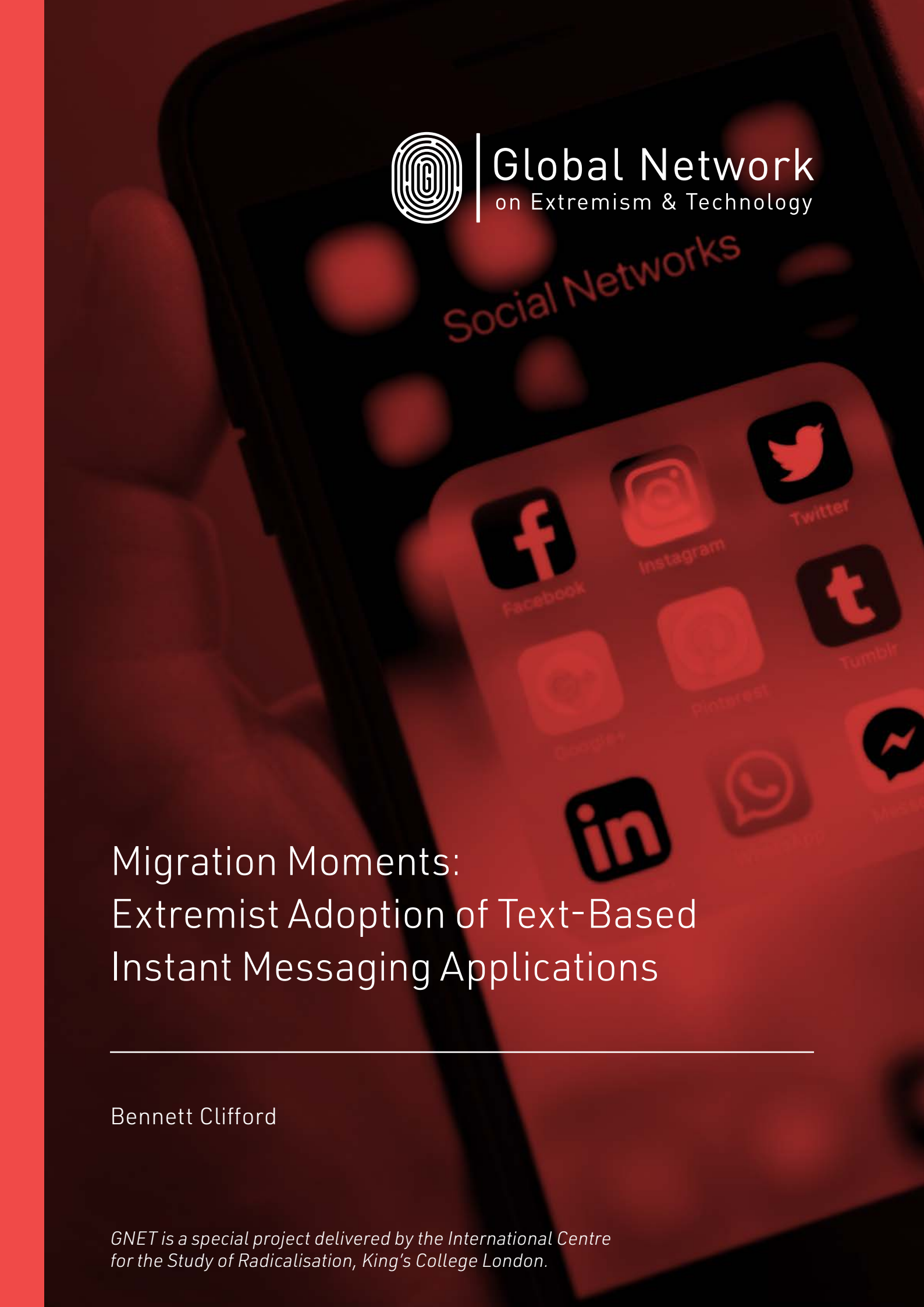

Migration Moments: Extremist Adoption of Text-Based Instant Messaging Applications

Bennett Clifford

GNET is a special project delivered by the International Centre for the Study of Radicalisation, King's College London.

The author of this report is Bennett Clifford, Senior Research Fellow, Program on Extremism at George Washington University

The Global Network on Extremism and Technology (GNET) is an academic research initiative backed by the Global Internet Forum to Counter Terrorism (GIFCT), an independent but industry-funded initiative for better understanding, and counteracting, terrorist use of technology. GNET is convened and led by the International Centre for the Study of Radicalisation (ICSR), an academic research centre based within the Department of War Studies at King's College London. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing those, either expressed or implied, of GIFCT, GNET or ICSR.

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

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

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.

Executive Summary

- Extremists of multiple persuasions – including jihadist supporters of al-Qaeda and Islamic State in Syria and Iraq as well as various extreme right-wing groups – currently use the text-based instant messaging application Telegram as a central coordinating forum for online activity. However, due to Telegram's new policies, collaboration with law enforcement and other industry partners, and increased enforcement of its terms of service, extremists are beginning to experience significant pressure to their Telegram-based ecosystem.

- Jihadists and far-right extremists online consistently experiment with other text-based instant messaging applications in conjunction with Telegram as potential alternatives. Nevertheless, a full-scale transition to another platform is unlikely in the short-term. In comparison to its competitors, Telegram's suite of features, familiarity to extremists and ease of use ensure that extremist exploitation of the platform will likely continue despite the company's new enforcement regimes.

- In conjunction with supporters of extremist groups' struggles to remain on Telegram, groups attempted to or plan to establish presences on other text-based instant messaging applications. In this regard, six platforms (BCM, Gab Chat, Hoop Messenger, Riot.im, Rocket.Chat and TamTam) drew significant attention from extremist groups during the past two years as potential alternatives to Telegram.

- The following analysis shows that extremists gravitated towards these platforms because of their suites of features, ease of use and host company's stances on privacy, security and regulation of extremist content.

- Two trends will likely chart the future of extremist exploitation of text-based instant messaging applications:

    - Supporters of extremist groups that established significant presences on Telegram are likely to seek out platforms with highly similar suites of features, affordances and visual layouts to Telegram.

    - Supporters of extremist groups will likely continue efforts to exploit text-based instant messaging platforms that offer decentralised servers and data storage.

- To counter extremist exploitation of text-based instant messaging applications, joint industry initiatives like the Global Internet Forum to Counter Terrorism may consider grouping text-based instant messaging service providers into individual forums for collaboration and information-sharing. More broadly, researchers, policymakers and practitioners of online counter-extremism should consider adopting a features-centric, as opposed to a platform-centric, approach to evaluating extremist exploitation of digital communications technologies.

Contents

1 Introduction: Extremists, Telegram, and Transition

This report examines the patchwork of online text-based instant messaging applications preferred by jihadist and far-right extremist groups, with a focus on charting their technical affordances and their host companies' stances on user privacy, security and regulation. To this end, the report analyses six online messaging services (BCM, Gab Chat, Hoop Messenger, Riot.im, Rocket.Chat and TamTam) that have been or may be used in conjunction with Telegram by extremist groups.

Currently, many supporters of various extremist groups are concentrated on the online instant messaging service Telegram, although some are attempting to make inroads to other platforms.[1] Telegram is consistently referred to as the "platform of choice" for jihadists online, most notably supporters of Islamic State in Iraq and Syria (IS), but it has also been continuously popular among extreme right-wing movements.[2] Analysts and scholars of online extremism, as well as many governments, consider Telegram a stable communications platform for extremist groups of multiple persuasions due to its suite of features, including end-to-end encrypted communications for its users and its guarantees of anonymity and privacy.[3] Extremists use Telegram channels and groups as staging grounds for a "multiplatform zeitgeist," wherein media content is rebroadcast from Telegram onto other messaging platforms and public-facing websites.[4]

However, recent changes to Telegram's terms of service and privacy policies are weakening the affordances the platform provides to extremist groups. For example, in April 2018, Telegram added Section 8.3 to its privacy policy. The section, a departure from Telegram's previous moratorium on information sharing with governments, states that "if Telegram receives a court order that confirms you're a terror suspect, we may disclose your IP address and phone number to the relevant authorities."[5] Concurrent with the change in its privacy policy, Telegram also began participating in "Referral Action Days" organised by Europol and individual European Union law enforcement agencies.[6] During the eleventh referral action day, the scope of Telegram's participation was merely to observe European law enforcement agencies' process for detecting and identifying terrorist content.[7]

1 Clifford, Bennett, and Helen Powell. 2019. "Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram." Washington, D.C.: Program on Extremism. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/EncryptedExtremism.pdf; Bloom, Mia, Hicham Tiflati, and John Horgan. 2017. "Navigating ISIS's Preferred Platform: Telegram." Terrorism and Political Violence 0 (0): 1–13. https://doi.org/10.1080/09546553.2017.1339695; Bloom, Mia, and Chelsea Daymon. 2018. "Assessing the Future Threat: ISIS's Virtual Caliphate." Orbis 62 (May). https://doi.org/10.1016/j.orbis.2018.05.007; "Telegram: The Latest Safe Haven for White Supremacists." 2019. Anti-Defamation League. 2 December 2019. https://www.adl.org/blog/telegram-the-latest-safe-haven-for-white-supremacists.

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

3 Clifford and Powell, "Encrypted Extremism".

4 *Ibid.*

5 *Ibid.*

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 October 2018. https://www.europol.europa.eu/newsroom/news/referral-action-day-six-eu-member-states-and-telegram.

However, during the sixteenth referral action day in November 2019, Telegram collaborated with Europol and industry partners Google, Twitter and Instagram.[8] Together, the platforms removed a total of 26,000 items of IS propaganda, including accounts, channels, groups, videos and other publications from their sites.[9] Commenting on the action, Belgian federal prosecutor Eric Van Der Sypt claimed that as a result of the mass takedown, IS "was not present on the internet anymore" for the time being.[10]

Despite Van Der Sypt's initial assessment, extremist groups retained a presence on Telegram after the referral action days. While the operation dealt a temporary blow to IS supporters on Telegram, Global Network on Extremism and Technology analyses found that "a stubborn remnant of its core presence" remained on the service, and "dissemination of both official and unofficial propaganda continues at a steady pace."[11] IS supporters, the only group known to have been targeted in the effort, quickly synthesised a presence on several alternate online instant messaging platforms. Through decentralisation, IS supporters were able to stay online as "dispersal to these dozen-plus platforms has further decentralized jihadist propaganda dissemination," but IS has "increased its exposure" by spreading the content across the web.[12] In July 2020, a Europol assessment declared that "efforts to establish an IS presence online are continuing across several platforms, including Telegram."[13] Officials involved in the Telegram referral action days commented that the efforts were largely focused on IS supporters, leaving other jihadist groups and other violent extremists largely unaffected by the crackdown.[14]

Throughout the takedowns of IS-related content on Telegram, far-right extremist groups sustained their large presence on the platform largely unimpeded by content removal efforts.[15] Yet this dynamic may be slowly changing. This summer, Telegram coordinated mass takedowns of prominent far-right extremist channels and groups on its platform.[16] The platform suspended some of the most violent and caustic right-wing extremist channels, including Terrorwave Refined, a "central hub" for the violent far-right on Telegram, as well as channels connected to the Misanthropic Division and RapeKrieg.[17] Despite the removals, most far-right channels on Telegram were unaffected and administrators of deleted channels continue efforts to post content on the platform.[18] It remains to be seen whether far-right extremists on Telegram will seriously consider the use of another platform or, indeed, whether Telegram's efforts will continue.

8 "Europol and Telegram Take on Terrorist Propaganda Online." 2019. Europol. 25 November 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 November 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 January 2020. https://www.flashpoint-intel.com/blog/terrorism/jihadists-presence-online-decentralizes-after-telegram-ban/.
13 "Online Jihadist Propaganda: 2019 in Review." 2020. Europol. 28 July 2020. https://www.europol.europa.eu/sites/default/files/documents/report_online_jihadist_propaganda_2019_in_review.pdf.
14 Amarasingam, "A View from the CT Foxhole."
15 Katz, Rita. 2020. "Neo-Nazis Are Running Out of Places to Hide Online." WIRED, 9 July 2020. https://www.wired.com/story/neo-nazis-are-running-out-of-places-to-hide-online/.
16 *Ibid.*
17 *Ibid.*
18 *Ibid.*

2 Text-Based Instant Messaging Applications: Categories of Analysis

A full-scale online extremist withdrawal from Telegram and mass migration to another platform is unlikely in the short term. Nevertheless, there is a need to understand alternative messaging platforms that extremist groups are using in addition to Telegram. Extremists do not make "either/or" decisions about platform usage; they frequently exploit multiple platforms at the same time.[19] Similar to extremists' experimentation with Telegram while Twitter and Facebook were still largely hospitable platforms, extremists are likely to experiment with secondary messaging platforms even if Telegram remains hospitable. Furthermore, analysis of these secondary platforms in comparison to Telegram can help demonstrate which types of features in messaging platforms are most attractive to extremist groups. Assuming that Telegram continues expansive and aggressive efforts to remove extremists from their platforms, it is necessary for practitioners to understand secondary platforms to contain second-order effects of takedown campaigns, such as extremist migration to platforms with weaker regulatory atmospheres, augmented affordances for extremists or privacy and security policies that occlude extremist messaging from law enforcement, intelligence or the platforms themselves.

The six platforms highlighted in this analysis obviously do not constitute an exhaustive list of the text-based instant messengers that extremist groups use today. However, they each have grappled with extremist exploitation of their services in recent years; comparison between the platforms can help reveal some of the critical affordances that are important for groups in selecting text-based instant messaging platforms. Specifically, this paper examines five factors for each platform that can determine its overall approach to extremist content: extremist usage, suites of features, user accessibility, privacy and security, and policy/regulatory landscape. Each of these five categories entails several key questions about the use of instant messaging platforms by extremist groups:

- *Extremist usage:* Which types of extremist groups use the platform? When did they begin using the platform? Are they currently using the platform? What is the extent of extremist usage of the platform?

- *Suite of features:* What features does this platform offer? Which of these features distinguish it from its competitors, especially when it comes to extremist (ab)use of the platform?

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

- *User accessibility:* How easy is it to use the platform? What steps are necessary to create an account and access specific content? What protocols does the system run on? Is the platform subject to disruptions, hacking attempts or other service denial efforts?

- *Privacy and security:* How do the platform's terms of service address user privacy? Does it offer encryption? Where does it store user data? Which third parties have potential access to user data?

- *Policy/regulatory landscape:* What is the platform's policy on removing terrorist and extremist content? Does it issue transparency reporting? Where is the platform registered and to which laws on content regulation is it subject? What is its relationship with government requests for user data?

In the final section, the report highlights the features that are most common across these platforms in an attempt to examine which features are most attractive to extremist groups. It also argues in favour of a features-specific, rather than a platform-specific, approach to analysing and countering extremist use of the internet.

3 Extremist Use of Secondary Text-Based Instant Messaging Applications

This section analyses six text-based instant messaging platforms that extremists have exploited or may exploit in the wake of Telegram's increased enforcement of its terms of service. Six months after the Telegram referral action days, a Europol report found that after a wave of takedowns, IS-affiliated jihadists online "flocked to TamTam and Hoop Messenger" while they tested out "marginal applications, such as the Blockchain messenger BCM, RocketChat and the free software instant messenger Riot."[20] Their counterparts in other jihadist groups, as well as in extreme right-wing groups, have also launched their own experiments on several of these platforms. In addition to these five platforms, the section analyses one additional platform, Gab Chat, that is currently in development but may be attractive to right-wing extremists due to its affordances and its host company's legacy.[21]

BCM Messenger 

BCM (Because Communication Matters) Messenger was a decentralised messaging application that offered both private chats and group chats for up to 100,000 participants.[22] While the company's origins are murky, the platform was created by Chinese developers and registered in the British Virgin Islands as a decentralised alternative to the Chinese messaging platform WeChat.[23] Several observers of online extremist media noted that IS supporters increasingly experimented with the application in the wake of the 2019 referral action days.[24] For instance, one of IS's major affiliate online media networks, Nashir News Agency, established several channels on the platform in December 2019.[25] In February 2020, the company notified users that it had discontinued its messaging service.[26]

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 July 2020. https://mashable.com/article/law-enforcement-documents-violent-white-extremists-encrypted-gab-chat/.
22 "BCM Messenger." n.d. BCM Messenger. Accessed 1 April 2020. "Privacy Policy," n.d. BCM Messenger. Accessed 1 April 2020. The BCM service is now discontinued. Accessible versions of the page and BCM's privacy policy can be found vin the Wayback Machine at https://web.archive.org/web/20200215082731/https://bcm.social/index.html and https://web.archive.org/web/20191016053505/https://bcm.social/license/policy.html.
23 *Ibid.*; Yuan, Lanny, Huaibing Jian, Peng Liu, Pengxin Zhu and ShanYang Fu. 2018. "AME Blockchain: An Architecture Design for Closed-Loop Fluid Economy Token System." White Paper.
24 Smith, Brenna. 2019. "Terrorists Use a New Blockchain Messaging App after Telegram Crackdown." Bellingcat CryptOSINT. 10 December 2019. https://mailchi.mp/7884c14d5fb9/terrorists-use-a-new-blockchain-messaging-app-after-telegram-crackdown.
25 *Ibid.*; Flashpoint, "Jihadists Presence Online Decentralizes After Telegram Ban"; Gluck, "Islamic State Adjusts Strategy to Remain on Telegram"; Webb, Sam, and Colin Rivet. 2019. "Terror Group ISIS Testing Blockchain Messaging App". 16 December 2019. https://finance.yahoo.com/news/terror-group-isis-testing-blockchain-150028142.html.
26 Message to BCM subscribers, 22 February 2020. https://postimg.cc/3dWTwGmp.

BCM distinguished itself from Telegram and other online instant messengers in several ways. First, and most importantly, it operated on a decentralised server model. Unlike other messaging services, which store user information and data on centralised servers controlled by the service provider, BCM and other decentralised platforms distributed the points of the server throughout the user network, allowing each user to store and control access to their own data.[27] While some online instant messengers provide end-to-end encryption for some (but not all) forms of communication or only provide it on request, messages sent through BCM were encrypted by default.[28] Otherwise, BCM was similar to Telegram in its suite of features (private and group chats) and the encryption algorithm it uses.[29]

To create an account in BCM, potential users could simply download the application and register a user ID. Unlike Telegram, a phone number was not required in order to register.[30] Accessing particular groups required a URL link to the content and contacting other users directly required knowing their BCM public key or user ID. BCM was based on a "decentralized infrastructure and application platform" called AME, which is designed on a principle of "zero trust": "the BCM app does not trust anyone except itself, not even the BCM Server."[31] Any third party, including the BCM server itself, was unable to decrypt messages sent between users. BCM also offers a cryptocurrency wallet in addition to its instant messaging service, which it still provides despite the shutdown of the messaging service.[32] As a result, some erroneously claimed that the instant messaging service was "blockchain-based," although only the digital wallet was based on the blockchain.[33]

According to BCM's privacy policy, the company "will not use or disclose [user data] to any third party without your prior permission."[34] Its decentralised platform and offer of default end-to-end encryption for all communications made it impossible for the company to decrypt messages between users. As user data is stored by individual nodes in the network, law enforcement request for access to servers would be highly difficult.[35] The company did not issue any guidance on how it planned to address terrorist or extremist content, but a company spokesperson commented that while it would follow laws in local jurisdictions, "under no circumstances will we compromise to any requests to provide decryption and back doors to content monitoring."[36]

Gab Chat

Gab was established in 2016 as a "free speech alternative" to Twitter; its co-founder, Andrew Torba, alleged a "left-leaning Big Social monopoly" as the main impetus behind creating the platform.[37] It gained notoriety as a coordinating point for far-right extremists online and drew scrutiny when the perpetrator of the October 2018 shooting at the Tree of Life

27 Yuan et. al. "AME Blockchain: An Architecture Design for Closed-Loop Fluid Economy Token System."
28 "FAQ." n.d. BCM Messenger. Accessed 1 April 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, "Privacy Policy."
35 *Ibid.*
36 *Ibid.*
37 Lorenz, Taylor. 2018. "The Pittsburgh Suspect Lived in the Web's Darkest Corners." The Atlantic. 27 October 2018. https://www.theatlantic.com/technology/archive/2018/10/what-gab/574186/.

Synagogue in Pittsburgh was found to have participated in a fringe community of neo-Nazis on the platform.[38] Since that time, several Gab service providers terminated their provision of services to the site.[39] After bouncing between service hosts, Gab has retained over 1,000,000 accounts and a steady community of right-wing extremists.[40]

In late January 2020, Gab announced that it was in the initial stages of rolling out an instant messaging platform similar to Telegram, called Gab Chat.[41] It bills the service as an "encrypted chat messaging service with public and private chat rooms."[42] Torba claimed that the public chatrooms would, like Telegram, not offer default encryption for all communications, but private chats would be end-to-end encrypted: "encrypted rooms cannot be read by anyone outside of the members in the chatroom, not even Gab."[43] Moreover, the app for Gab Chat would only be hosted on Gab's website rather than on popular app stores provided by Google and Apple.[44]

The primary advantage of Gab as a platform for extremists is a guarantee by the company against content moderation and removal. It views the provision of free speech as sacrosanct and prides itself on its policy against censorship.[45] However, "in the event that an unlawful threat is detected on the platform, or we become aware of serious violent off-platform conduct by an individual who may have created an account on our site," the company will "[cooperate] and [communicate] with federal, local, and state law enforcement frequently … to assist with the interdiction of serious crime."[46]

Gab Chat is still in beta.[47] However, given the popularity among right-wing extremists of Gab as an alternative to public-facing social media providers like Twitter and Facebook, it is reasonable to expect that some extremist adoption of Gab Chat will occur. This is compounded by the popularity of Telegram and Telegram-like services by right-wing extremists. If Gab Chat provides similar services as Telegram under the Gab banner, far-right extremists may consider it a hospitable online instant messaging platform and attempt to exploit the platform when it is fully functional.

Hoop Messenger

Hoop Messenger is an online instant messaging application that, similar to Telegram, provides communication options in the forms of private chats, chatrooms and one-to-many channels. The service is operated by a small company in Canada.[48] In December 2019, following the Europol-coordinated takedown efforts of IS-related media,

38 *Ibid.*
39 Jurecic, Quinta. 2018. "Gab Vanishes, and the Internet Shrugs." Lawfare. 29 October 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 March 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 January 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 August 2019. https://news.gab.com/2019/08/23/gabs-policies-positions-and-procedures-for-unlawful-content-and-activity-on-our-social-network/.
46 *Ibid.*
47 Torba, "AG Barr is Wrong on Encryption."
48 "FAQ." n.d. Hoop Messenger. Accessed 1 April 2020. http://hoopmessenger.com/faq/.

several official and unofficial IS and al-Qaeda media outlets set up channels on Hoop Messenger, with some supporters encouraging the use of the platform as a secure alternative to Telegram.[49] Several days later, however, the company removed a large number of IS-related channels on its platform.[50] In late January 2020, a pro-IS media foundation warned its followers against using Hoop Messenger, claiming that it collects extensive personal information from users.[51]

Today, a substantial IS presence remains on Hoop Messenger. From some notable IS supporters' perspectives, it may currently be the most attractive option as a Telegram alternative. In early June 2020, a Nashir News Agency channel on Telegram issued an "urgent" message to its followers that Hoop Messenger would be its primary channel for news dissemination.[52] This announcement came in the wake of continued pressure against pro-IS channels on Telegram. In the days following the announcement, supporters imported a significant number of pro-IS channels from Telegram to Hoop Messenger.[53] The IS-affiliated Electronic Horizons Foundation, responsible for producing content on digital and operational security, issued a manual to its subscribers on how to use Hoop Messenger safely.[54] Despite these efforts, Hoop Messenger responded in turn, launching another campaign to remove pro-IS content from its platform.[55]

The feature that distinguishes Hoop Messenger from other instant messaging services is "the Vault", a password-protected file storage system where users can save chats, photos, videos and other files. Once a user creates a password, all chats and files saved within the Vault are end-to-end encrypted on both the user's device and the cloud; otherwise, channels and all other chats are not end-to-end encrypted.[56] Users can also create fake passwords for their Vault that when entered, would cause the contents of the Vault to self-destruct.[57] Through the service's website, users also have the option of remotely deleting their account, which permanently deletes all data on a user's account and personal data stored on their phone.[58] According to the company, the Vault's dummy passwords and self-destruction are especially useful when "you enter areas that demand that you hand in your phone … simply delete Hoop and download it again once it is safely back in your hands."[59]

---

49 Amarasingam, Amarnath. 2019. "Telegram Deplatforming ISIS Has Given Them Something to Fight For." Vice. 5 December 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 December 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 December 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 January 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 June 2020. https://www.memri.org/cjlab/isis-media-outlet-announces-shift-canadian-hoop-messenger-app-after-wave-account-deletions.

53 *Ibid*.

54 Gluck, Raphael. 2020. "Among AFAQ's recent offerings – A tutorial on how to safely use Hoop Messenger – ISIS' new go to app following sustained Telegram deletions. – "The Supporters Security" magazine, raising security awareness among keyboard warriors – Debian video tutorial." Tweet, 3 July 2020. https://twitter.com/einfal/status/1279124715957891072.

55 Alkhouri, Laith. 2020. "Multiple official and unofficial #ISIS channels have been removed from the group's favorite communications/propaganda platform Hoop Messenger. This, however, has had very little impact on the group's media distribution as it has created dozens of backup channels early on." Tweet, 6 August 2020. https://twitter.com/MENAanalyst/status/1291415487453302790.

56 Hoop Messenger, "FAQ".

57 *Ibid*.

58 *Ibid*.

59 "Hoop Messenger." n.d. Hoop Messenger. Accessed 1 April 2020. http://hoopmessenger.com/.

Creating an account in Hoop Messenger requires registration with a phone number and/or email address. Unlike some other platforms, users can create multiple user IDs on the same account.[60] Opt-in is required for chats to receive end-to-end encryption, which can only be done through the Vault, but Hoop Messenger also provides a built-in virtual private network (VPN) browser in its service so users can browse the web from the application without being monitored.[61] The layout and functionality of the platform are similar to Telegram.

Sections 9, 10, and 11 of Hoop Messenger's terms of service dictate the service's approach to harmful content. The service prohibits "objectionable behavior and content unacceptable to us," and notes that the company will remove any content or user account that violates the terms of service.[62] In December 2019, the company clarified that these procedures apply to terrorist content and claimed that the company "will continue shutting down ISIS-related groups" after deleting a significant number of pro-IS channels and chats on the platform.[63] Due to the company's concerted action against IS-related content and accounts, some supporters appear to have moved away from using Hoop Messenger, issuing warnings against its use.[64] Nevertheless, other IS supporters remain convinced that the platform is its most viable alternative to Telegram.

Riot.im

Riot.im is a decentralised chat application based on the Matrix network.[65] It provides communications in the form of one-to-one chats and groups, some file-sharing functionality and gives users a choice about access control to communications.[66] It was initially designed as an office collaboration platform and structurally resembles other instant messaging applications in that category (e.g. Slack, Twist, Microsoft Teams).[67] During a period of experimentation with decentralised web platforms, IS supporters first started establishing groups on the platform in September 2017, and al-Qaeda and other jihadist supporters followed shortly thereafter.[68] These groups have consistently maintained a presence on the platform since 2017.[69] However, as most supporters elected to store the communications on the company's public server, there are constant disruptions to jihadist networks on Riot.im servers due to content removal and account removal efforts.[70] Observers of right-wing extremist groups online also note that some prominent right-wing extremist channels on Telegram are also beginning to establish a presence on Riot.im.[71]

60 *Ibid.*
61 *Ibid.*
62 "Privacy & Terms." n.d. Hoop Messenger. Accessed 1 April 2020. http://hoopmessenger.com/legal/.
63 @HoopMessenger, 2019. "We will continue shutting down ISIS-related groups. We encourage everyone to send us suspicious channels via email. Since our team is quite small we are relying on the public to help us. If there are any questions please reach out to our team via email or DM." 5 December 2019. https://twitter.com/HoopMessenger/status/1202698188160811008.
64 MEMRI, "Pro-ISIS Media Foundation Warns ISIS Supporters Against Using Hoop Messenger."
65 "Features." n.d. Riot.im. Accessed 1 April 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 with Jon Lewis, Program on Extremism, 1 April 2020.

Due to its foundation on the decentralised Matrix platform, observers of online extremist activity were concerned that Riot.im "could become the next enhanced version of Telegram" if extremists chose to host their own servers.[72] As an option, Riot.im offers users a choice between storing their communications on the matrix.org public server, on a premium, paid server hosted by the individual user (or their organisation), on other public servers created by Riot.im users or on custom servers.[73] Thus, while the platform offers decentralised servers, it requires the individual user to opt-in and then manage the server. Regardless of whether communications are stored on a centralised, public server or a decentralised one, users can enable end-to-end encryption for their communications on Riot.im.[74]

Registering for a Riot.im account requires the creation of a username and password, and users can also elect to provide an email address.[75] Following account creation, the owner of a chat can change its settings so that only select users can participate, so that only users with a URL link to the chat can access it, or the chat is made public.[76] Participants can also enable end-to-end encryption for messages.

Riot.im is built on the Matrix platform and its public servers are hosted on Matrix. Both services are based in the United Kingdom.[77] The relationship between Riot.im and Matrix has notable implications for how extremists perceive privacy and security on the platform. First, extremist users of Riot.im often choose to host communications on the default Matrix public servers, as opposed to creating and managing their own decentralised servers.[78] This means that their communications are covered by Matrix's terms of service and subject to strict regulations on extremist online content in the United Kingdom. Matrix's terms of service prohibit the use of the service "for any unlawful purposes or in support of illegal activities under UK/EU law," including terrorist content.[79] The company thus routinely takes down extremist content and accounts from its platforms. When extremist groups host content on decentralised, third-party servers, they often encounter patchy service and independent takedown efforts by small-platform owners.[80] To date, few extremists have taken the initiative to host Riot.im chats on self-managed servers.[81]

Rocket.Chat

Rocket.Chat is a decentralised online instant messaging platform that offers its users the ability to host content and communications on their own servers or store material on the public Rocket.Chat server.[82] Notably, in December 2018, IS's central media experimented with managing its own server for communications on Rocket.Chat, one of the first attempts by jihadists to take full advantage of decentralised

72 Bodo, Lorand. 2018. "Decentralised Terrorism: The Next Big Step for the so-Called Islamic State (IS)?" VOX – Pol. 12 December 2018. https://www.voxpol.eu/decentralised-terrorism-the-next-big-step-for-the-so-called-islamic-state-is/.
73 Riot.im, "Features".
74 *Ibid*.
75 *Ibid*.
76 *Ibid*.
77 "Privacy Notice." n.d. Riot.im. Accessed 1 April 2020. https://riot.im/privacy.
78 King, "Islamic State Group's Experiments with the Decentralized Web".
79 Riot.im, "Privacy Notice".
80 King, "Islamic State Group's Experiments with the Decentralized Web".
81 *Ibid*.; Bodo, "Decentralized Terrorism".
82 "Rocket.Chat." n.d. Rocket.Chat. Accessed 1 April 2020. https://rocket.chat/.

web platforms.[83] IS's Nashir News Agency hosted several Rocket.Chat channels on a server called Techhaven, whose user guide claimed it was designed to provide "an open forum for discussion, digital privacy and innovation to oppressed users in conflict zones who are targeted for their beliefs by the authoritarian regimes of the West."[84] Since then, IS and other jihadist groups, including al-Qaeda, have set up channels and groups on Rocket.Chat.[85]

Of the other platforms examined in this report, Rocket.Chat is most similar to Riot.im in that they are messaging platforms initially designed for office workstream collaboration that offer users the choice between centrally administered servers and user-managed, decentralised servers.[86] It is easier to create and manage a server on Rocket.Chat than on Riot.im. Establishing an account on the public Rocket.Chat server or signing up for a privately hosted server requires a username, password and email.[87] Once an account is established, users can directly chat with other users or create public or invitation-only channels. The platform also includes several other unique features that are potentially attractive to extremist groups, including automated translation of posts between languages.[88]

The option to host decentralised servers represents a conundrum for extremist groups. If they choose to host Rocket.Chat communications on the company's central server, the company can either remove channels that are promoting extremism pursuant to the user code of conduct or, if circumstances apply, the company is "required to disclose your Personal Data if required to do so by law or in response to valid requests by public authorities."[89] Choosing to host communications on a decentralised server can be time-consuming. It requires some technical expertise and can pose other problems for extremist groups.[90] Three months after Nashir News Agency established its channels on the Techhaven server, the host was targeted by distributed denial of service attacks that rendered most of their Rocket.Chat channels inoperable.[91] Creating a specially designated server to host extremist propaganda can place a digital target on the server's back. In the event of a successful disruption, extremist groups on decentralised platforms such as Rocket.Chat can be forced to jump from server to server, limiting the utility of the platform as a stable base for propaganda.

TamTam

TamTam is an online instant messenger managed by the Mail.ru Group, the Russian firm that holds the largest share of the Russian-speaking internet and also operates the popular social media platforms Vkontakte and Odnoklassniki.[92] TamTam is almost structurally identical to Telegram in terms of its suite of features. It offers chats, public

83 BBC News. 2019. "Europol Disrupts IS Propaganda Machine." 25 November 2019, sec. Middle East. https://www.bbc.com/news/world-middle-east-50545816.
84 King, "Islamic State Group's Experiments with the Decentralized Web".
85 Flashpoint, "Jihadists Presence Online Decentralizes After Telegram Ban".
86 Rocket.Chat, "Rocket.Chat".
87 *Ibid.*
88 *Ibid.*
89 "Rocket.Chat Privacy Policy." n.d. Rocket.Chat. Accessed 1 April 2020. https://rocket.chat/privacy.
90 King, "Islamic State Group's Experiments with the Decentralized Web".
91 *Ibid.*
92 "Some Messenger Called 'TamTam' Is Trying to Replace Telegram in Russia. What the Heck Is It?" 2018. Meduza. 17 April 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.

channels, private channels and group chat options.[93] The similarity between Telegram and TamTam is intentional. TamTam was created as a Telegram alternative by the Mail.ru Group during ongoing efforts by Russia's government to block Telegram IP addresses from the Russian internet.[94] The Mail.ru Group has close ties to the Russian government and is allegedly more willing to accede to Russian law enforcement requests for user information than its counterpart.[95]

Supporters of IS established a sizable number of channels and groups on TamTam following the December 2019 Europol-coordinated action on Telegram.[96] TamTam quickly acted against the uptick in IS-related content.[97] A company spokesperson told Vice News that TamTam is "strongly against the presence of any sort of content by terrorist organizations on our platform" and called on users to report content and accounts promoting terrorist groups.[98] After TamTam's purge, jihadist groups began cautioning their followers not to use the platform.[99] For instance, in February 2020, a group of English-speaking IS supporters named "Lions of Tawheed" posted on Rocket.Chat that "the Russian government has access to all TamTam accounts … protect yourself by removing TamTam from your phone or computer. Use secure applications like Riot, Rocket.Chat and Telegram."[100]

TamTam requires users to follow the same procedures as Telegram for creating an account and accessing content. It offers the same suite of features as Telegram, including options for one-to-one chats, one-to-many channels and large group chats.[101] Users can make chats and channels publicly accessible or privately accessible through invitation.[102] TamTam's similarities to Telegram extend even to its domain name. Telegram's shortened hyperlinks are accessed through the domain name t.me; TamTam's use tt.me.[103] The company actively promotes its interoperability with Telegram on the Russian market by openly advertising how similar it is to Telegram on popular Russian Telegram channels.[104]

The major difference between Telegram and TamTam is in the area of privacy and security. TamTam is registered in the Russian Federation and its data policy is "processed in accordance with the laws of the Russian Federation."[105] This means that TamTam, unlike Telegram, actively adheres to the Russian law that requires service providers to grant backdoor access to the Federal Security Service (FSB), the main law enforcement agency in the Russian Federation.[106] While it purports to offer encryption, experts believe that it may have handed over copies of TamTam encryption keys to the FSB.[107] TamTam's license

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 December 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 March 2020. https://www.memri.org/cjlab/pro-isis-outlet-lists-safe-messaging-apps-advises-against-using-chinese-russian-apps.
100 *Ibid*.
101 "About TamTam." n.d. TamTam. Accessed 1 April 2020. https://about.tamtam.chat/en/index.html.
102 *Ibid*.
103 Meduza, "Some Messenger Called 'TamTam' Is Trying to Replace Telegram in Russia."
104 *Ibid*.
105 "TamTam Messenger Confidentiality Policy." n.d. TamTam. Accessed 1 April 2020. https://about.tamtam.chat/en/policy/index.html.
106 *Ibid*.
107 *Ibid*.

agreement explicitly prohibits users from "[propagating] extremism, terrorism, excite [*sic*] hostility based on racial, ethnical or national identity" or publishing "information of extremist nature."[108] It is reasonable to assume that while IS supporters attempted to exploit TamTam in the wake of the 2019 Europol referral action days, they chose TamTam because of its similarity to Telegram as opposed to its privacy and security features.

108 "TamTam Messenger End User License Agreement." n.d. TamTam. Accessed 1 April 2020. https://about.tamtam.chat/en/license/index.html.

Figure 1: Comparison of Text-Based Instant Messaging Platforms used by Extremist Groups

Platform	Extremist usage	Country of registration	Suite of features	Security	Policy/regulatory environment
Telegram	Jihadist (IS, al-Qaeda), Far-Right	British Virgin Islands/ United Arab Emirates	• One-to-one chats • Group chats • Public and private chats	• End-to-end encryption for one-to-one chats • Account/data self-destruct	• Will remove "terrorist" public content (bots and public channels) • If ordered by a court, will provide user information to law enforcement agencies in terrorism-related cases
BCM*	Jihadist (IS)	British Virgin Islands	• One-to-one chats • Group chats	• End-to-end encryption • Account/data self-destruct • Decentralised server option	• No known policy on extremist content removal or moderation • No third-party disclosure of user data to law enforcement
Gab Chat**	Far-Right	United States of America	• One-to-one chats • Group chats	• End-to-end encryption on device • Message deletion on server after 30 days	• "Offensive" and "hateful" speech not grounds for content removal, only "illegal content and activity" • Will cooperate with US government on lawful requests for user data during investigation, not other governments or third parties
Hoop Messenger	Jihadist (IS, al-Qaeda)	Canada	• One-to-one chats • Group chats • Public and private channels	• End-to-end encryption on all chats and files in password-protected "Vault" • Remote deletion of accounts and content in the Vault	• Company "will remove Content that we find, in our sole discretion, unlawful, obscene, offensive, threatening, libellous, defamatory or otherwise objectionable"

Platform	Extremist usage	Country of registration	Suite of features	Security	Policy/regulatory environment
Riot.im	Jihadist (IS, al-Qaeda), Far-Right	United Kingdom	• One-to-one chats • Group chats	• End-to-end encryption enabled by user • Decentralised server option	• Company can remove content on public servers supporting "any unlawful purposes or in support of illegal activities under UK/EU law"
Rocket. Chat	Jihadist (IS, al-Qaeda)	United States of America/ Brazil	• One-to-one chats • Group chats • Public and private channels	• End-to-end encryption enabled by user • Decentralised server option	• Company is "required to disclose your Personal Data if required to do so by law or in response to valid requests by public authorities"
TamTam	Jihadist (IS, al-Qaeda)	Russian Federation	• One-to-one chats • Group chats • Public and private channels	• "Encryption" (unclear protocol)	• Company prohibits propagating "extremism, terrorism, excite [*sic*] hostility based on racial, ethnical or national identity" or publishing "information of extremist nature" • "Users' data shall be processed in accordance with the laws of the Russian Federation," which entails mandatory disclosure of information and encryption keys to Russian law enforcement

* Service discontinued, February 2020
** Currently in beta

4 Analysis: The Extremist Adoption Curve for Text-Based Instant Messaging Applications

Extremists' experimentation with text-based online instant messaging services is an important facet of their efforts to adopt emerging technology. In the wake of difficulties on Telegram, extremist adoption of secondary messaging applications generally follows what Daveed Gartenstein-Ross, Matt Shear and David Jones have referred to as the "violent non-state actor (VNSA) technology adoption curve."[109] In the initial stages of early adoption, extremists make (usually failed) attempts to harness emergent technology.[110] In the iteration stage, they begin to improve their ability to use the technology, while new products come onto the market that aid their endeavours.[111] After iteration, extremist groups may experience a breakthrough – landing on a particular method for using the technology that greatly augments their strategies.[112] However, extremist groups inevitably face competition in the form of governments' and service providers' responses.[113] Significant competition can restart the adoption curve, this time for substitutes to the original technology as extremist groups are forced to experiment with the early adoption of new technologies.[114]

The breakthrough that extremists achieved in the 2015–17 period with the use of Telegram is arguably transitioning into the competition stage. During the past year, Telegram, in conjunction with government agencies, began to contest extremist use of the platform significantly. This caused extremists of several variants to restart the early adoption stage for the use of several Telegram substitutes.[115] With the VNSA technology adoption curve as a guide, we can assess that most current efforts by extremist groups to find a sustainable and secure alternative to Telegram have been unsuccessful. Yet extremist groups have an established track record of quick organisational learning when it comes to adopting new social media platforms.[116] With the emergence of increasingly stable instant messaging platforms offering new privacy and security features, extremists making the jump from Telegram to a secondary instant messenger raises questions of "when" and "which", not "if".

109 Gartenstein-Ross, Daveed, Matt Shear and David Jones. 2019. "Virtual Plotters. Drones. Weaponized AI?: Violent Non-State Actors as Deadly Early Adopters." Washington, D.C.: Valens Global. http://valensglobal.com/wp-content/uploads/2019/11/VNSAs-as-Deadly-Early-Adopters-for-web-publication_1.pdf.
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".
116 Shapiro, Jacob N. 2015. The Terrorists Dilemma: Managing Violent Covert Organizations. Reprint edition. Princeton University Press; Kenney, Michael. 2010. "Beyond the Internet: Mētis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists." Terrorism and Political Violence 22 (2): 177–97. https://doi.org/10.1080/09546550903554760; Gartenstein-Ross et al., "Virtual Plotters. Drones. Weaponized AI?"; Alexander, "Digital Decay."

Different groups of extremists will likely transition away from Telegram at different times, as they currently face disparate competition on the platform. The measures in effect against extremists on Telegram from the company and governments, from content and account takedowns to monitoring efforts, largely focus on IS supporters.[117] Meanwhile, supporters of other extremist groups, including far-right extremists and other jihadist groups, face limited contestation and therefore less incentive to move away from the platform.[118] For this reason, IS supporters will likely continue to drive efforts to experiment with emergent instant messaging platforms as wholesale alternatives to Telegram. However, if Telegram begins substantial crackdowns on other types of extremist activity on its platform, a wider range of jihadists and extreme right-wing groups may follow suit.

A preliminary assessment based on the platforms listed above can highlight some of the features that extremist groups may be looking for in adopting Telegram substitutes. Notable similarities and trends appear within this group of instant messaging applications that extremist groups have adopted in the wake of increased competition on Telegram. First, many offer very similar communication options and layouts to Telegram. It is no coincidence that in the days following the Europol referral action days, one of the first platforms on which IS supporters established a following was TamTam.[119] The application is a near carbon copy of Telegram, even advertising itself as such. Despite negligible security and privacy features, it instantly attracted extremist Telegram users because of its similarity to the platform. In the early stages of finding a Telegram substitute, similarity to Telegram was considered an advantage for extremist groups because supporters could quickly adapt to the new platform, ensuring ease of use and familiarity.

The analysis above also shows that extremist groups are increasingly experimenting with instant messaging platforms that offer decentralised servers and data storage. So far, most groups seem to have not taken full advantage of the option to decentralise data storage while using such platforms as BCM, Riot.im, or Rocket.Chat.[120] Managing independent servers for these platforms can be time-consuming, resource-intensive and – as the Nashir News Agency found when it attempted to establish a decentralised Rocket.Chat server for its propaganda channels – create additional targets for governments, competitors and independent hackers.[121] Initial rollouts of these platforms and rudimentary extremist efforts to exploit them face glitches, service denials and other technological issues. However, new platforms, like ZeroNet, Matrix and others, are making decentralised server-hosting much easier for consumers, which will inevitably make these platforms more accessible to extremist groups.[122]

117 Amarasingam, "A View from the CT Foxhole"; Conway, Maura, Moign Khawaja, Suraj Lakhani, Jeremy Reffin, Andrew Robertson and David Weir. 2019. "Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts." Studies in Conflict & Terrorism 42 (1–2): 141–60. https://doi.org/10.1080/1057610X.2018.1513984; Conway, Maura, Ryan Scrivens and Logan Macnair. 2019. "Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends." The Hague, Netherlands: International Centre for Counter-terrorism. https://icct.nl/wp-content/uploads/2019/11/Right-Wing-Extremists-Persistent-Online-Presence.pdf.
118 Amarasingam, "Telegram Deplatforming ISIS Has Given Them Something to Fight For".
119 King, "Islamic State Group's Experiments with the Decentralized Web"; Bodo, "Decentralized Terrorism".
120 *Ibid*.
121 *Ibid*.
122 *Ibid*.

Nevertheless, an instant messaging platform built on the decentralised web may be a good candidate as an application to replace Telegram, especially if it becomes readily available to extremists and easy to use. Lorand Bodo writes that "the decentralized web seems to be the next logical step not only for IS, but also for other (violent) extremists online trying to evade authorities and take-downs."[123] The motivation for adopting decentralised web platforms is simple: extremists online face threats both from governments attempting to surveil, identify and interdict potential terrorists and from tech providers attempting to eliminate the presence of extreme propaganda on their platforms.[124] Through Telegram and other services, extremists are now adept at using privacy-maximising services like end-to-end encryption, but face an uphill battle in maintaining network resilience on platforms.[125] If groups are able to store data on their own servers, this in effect would mitigate the effect of tech companies' content removal efforts by creating an independent, decentralised storage network outside the grasp of service providers.[126]

123 Bodo, "Decentralized Terrorism".
124 *Ibid.*
125 *Ibid.*
126 *Ibid.*

5 Recommendations: Towards a Features-Centric Approach to Online Extremism

The prevalence of Telegram-like messengers and decentralised applications within the chat apps exploited by extremists in the wake of increased competition on Telegram underscores that applications' suites of features are critically important for adoption. In turn, it behoves online counter-extremism policy to shift away from focusing on specific platforms or applications and instead adopt a features-centric approach to extremists' exploitation of digital communications technologies. Research and policymaker attention is intensely focused on a select number of "problem" platforms – in recent years, Twitter and Telegram – while it ignores a broader ecosystem of online extremist communications.[127] This dynamic plays out in online targeted action raids like the Europol referral action days, which have led some policymakers to frame content removal on specific platforms as total victories against online extremism. As this paper demonstrates, the resultant decentralisation of platform use can circumvent the positive effects of these operations.[128]

Overall, a features-centric approach would benefit online counter-extremism by matching policyresponses to the ways that extremists conceptualise their use of the internet. Additionally, by focusing on countering extremist exploitation of features as opposed to platforms, service providers can more easily find kindred companies to share responses and innovation. Data from multiple studies of specific platforms suggest that extremists gravitated towards these applications not because of brand name or legitimacy but because of the features offered.[129]

In response to extremist exploitation of the internet, European and American policymakers with regulatory authority tend to single out particular platforms and target them with regulatory pressure, targeted disincentives and ultimatums. In some cases, these actions may be necessary. Unfortunately, there exist platforms with incredibly poor track records with regard to online extremism due to failure to enforce terms of service, severe capacity gaps, poor regulatory environments or even biases towards particular extremist groups that prevent them from action. Singling out these platforms is necessary for regulatory enforcement. However, widespread extremist exploitation also occurs on platforms that, despite good-faith efforts to moderate and/or remove content, are attractive to extremists because of their suites

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

of features or their reach into mass audiences. A features-centric approach that evaluates extremists' exploitation of specific affordances across platforms would help policymakers distinguish between platforms with governance and moderation issues, which may respond well to pressure, and those that are simply attractive to extremists for their features, which may not.

For online counter-extremism bodies such as the Global Internet Forum to Counter Terrorism (GIFCT), grouping similar platforms together could help partners tailor overarching, holistic objectives of countering extremism to specific features shared among the platforms. Ali Fisher, Nico Prucha and Emily Winterbotham write that "focusing on the multiplatform communication paradigm rather than individual platforms is key to the future development of a next-generation approach to online disruption."[130] Sharing of best practices, responses and ideas between platforms offering similar features, such as file-sharing platforms, instant messengers or social media sites, allows for improved collaboration and innovation. This can augment existing information-sharing, such as URL hash-sharing databases, by allowing various platforms to trace the spread of extremist content from one platform to another.[131]

Finally, and most importantly, greater collaboration among platforms with similar features can serve as an early warning system for extremists transitioning between platforms. As an example, an instant messaging platform that is linked into an information-sharing consortium with other platforms has a direct channel to notify others when it is planning aggressive action to take down extremist content and networks on its platform. The other instant messaging platforms, receiving advanced notification that extremists may consider shifting to their services as a result, can proactively prepare responses. The potential for service providers to disrupt the process of extremist adoption of new platforms in the early iteration stage could severely hamper how quickly and easily extremists establish launching points on new platforms.

As the GIFCT expands membership to new companies in the coming years, it should consider combining its current broad-based avenues for collaboration with more limited working groups that gather specific categories of service providers together. While this paper shows that this model of collaboration could be useful for instant messaging platforms, more research and experimentation could determine whether other types of service providers, such as social media, file-sharing or e-commerce could benefit from features-specific groupings within GIFCT. By taking the lead, this approach within GIFCT could also guide policymakers and researchers towards carefully evaluating the role of suites of features in extremist adaptation, tailoring their policy responses and research to include broader swathes of the online extremist ecosystem. In sum, the features-specific paradigm could assist technology companies, policymakers, practitioners and researchers to flatten the curve of extremist adaptation of digital communications technologies.

130 Fisher et al. "Mapping the Jihadist Information Ecosystem".
131 *Ibid*.

Policy Landscape

This section is authored by Armida van Rij and Lucy Thomas, both Research Associates at the Policy Institute based at King's College London. It provides an overview of the relevant policy landscape for this report.

Introduction

Terrorists' use and abuse of the internet has long challenged policymakers, law enforcement agencies and technology companies alike. On the one hand there are the very public cases of misuse of technology: the live streaming of a terrorist attack in New Zealand is a prime example. But another potential problem is terrorists or terrorist organisations using private messaging applications to plan and recruit for their activities. The use of end-to-end encrypted messaging apps has grown among terrorist organisations, precisely because they offer a private means of communications, not easily accessible by law enforcement agencies. This problem has grown in recent years for the messaging app Telegram, but also for newer alternatives to Telegram, as terrorists seek out alternatives to hide from law enforcement.

This report will set out some of the key challenges facing national governments in tackling end-to-end encrypted messaging apps. For nine countries, it will set out key legislation and stakeholders and the challenges policymakers face when seeking to prevent the misuse of messaging apps, as well as the challenges law enforcement faces during its investigations because of the encryption. It will also discuss the challenges posed by the move towards decentralised messaging platforms and possible approaches to governing them.

IM Applications and CVE: Addressing the Challenges and Assessing New Developments

Canada

The Canadian government's counterterrorism and counter-radicalism strategy is expansive, encompassing traditional intelligence and security agency activities, engagement with civil society, collaborative initiatives with industry and community-focused policing. Its strategy, as laid out in its National Strategy on Countering Radicalization to Violence, has three main strands of direction: to develop counter-messaging with civil society, to support countering violent extremism (CVE) research and to partner with international initiatives and tech companies.[132]

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

Canada has perhaps the most developed counter-messaging and civil-society-focused strategy of all the jurisdictions under review here. Extreme Dialogue is a counter-messaging initiative between the Canadian government and the Institute of Strategic Dialogue. The project provides educational resources to practitioners and young people through films that illustrate the negative impact of extremism.[133] The Canada Centre for Community Engagement and Prevention of Violence houses a number of community-based interventions to counter radicalisation to violence. In Calgary, for instance, the ReDirect programme works with the Calgary Police Service and the City of Calgary Community & Neighborhood Services, as well as health and social services agencies to intervene in the early stages of radicalisation. ReDirect employs a range of strategies including referral, education and providing advice for individuals seeking a way to leave a violent extremist group.[134]

In terms of supporting CVE research, in 2019 Canada commissioned Tech Against Terrorism, an international UN-sponsored initiative that works with the global tech industry, to develop a Terrorist Content Analytics Platform (TCAP), a database that hosts verified terrorist material and content from existing datasets and open sources.[135] The platform has the ability to act as a live alert facility for smaller internet platforms who may not have the capacity or resources to comply with regulatory efforts to take down malicious and extremist content.

Lastly, Canada is party to a range of international and cross-sector initiatives. Following the Christchurch mosque attacks in March 2019, Prime Minister Justin Trudeau joined the Christchurch Call to Action, a joint commitment between governments and the tech industry to "eliminate terrorist and violent extremist content online."[136] Alongside co-sponsoring technical developments to help track and take down extremist content – such as the GIFCT hash database[137] – the call to action also commits governments to support frameworks, capacity-building and awareness-raising activities in order to prevent the use of online services to disseminate terrorist and violent extremist content.

European Commission

Within Europol sits the European Counter Terrorism Centre (ECTC), established following the 2015 attack on the staff of satirical magazine *Charlie Hebdo* in Paris, as proposed in the European Commission's European Agenda on Security. The purpose of the ECTC is to "improve the exchange of information and the operational support to Member States' investigators".[138] The Commission also launched the EU Internet Forum in 2015, which brings together governments, Europol and technology and social media firms to ensure illegal content is taken down as quickly as possible.[139]

133 See: https://extremedialogue.org/
134 See: http://redirect.cpsevents.ca/
135 The TCAP has also been covered in the Policy Landscape section of a GNET report on 'Decoding Hate: Using Experimental Text Analysis to Classify Terrorist Content.' Accessed via: https://gnet-research.org/wp-content/uploads/2020/09/GNET-Report-Decoding-Hate-Using-Experimental-Text-Analysis-to-Classify-Terrorist-Content.pdf
136 See: https://www.christchurchcall.com/
137 See: https://www.gifct.org/joint-tech-innovation/
138 European Commission, Migration and Home Affairs, *Counter-terrorism and radicalisation*. https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism_en
139 European Commission, Press Office, *EU Internet Forum: Bringing together governments, Europol and technology companies to counter terrorist content and hate speech online*. 3 December 2015. https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6243

The European Commission recognises that it is not only the big technology firms that are used and abused by terrorist organisations, but also smaller providers who offer "different types of hosting services".[140] Secure encryption and accessing private data has proven a challenge for law enforcement during investigations.

Europol has launched several big operations to remove IS and IS-affiliated users from Telegram. Over the course of several days in November 2019, Europol took down a total of 5,055 accounts and bots, compared to a daily average of 200 to 300 account takedowns at other times.[141] In December 2018, 3,276 accounts were taken down in a single day, according to Telegram, and Europol had another such day earlier that year in April.[142] While these single events significantly disrupt IS operations, it is unlikely to have a lasting impact unless clampdown efforts are consistent.

In parallel to these clampdown days, a collaboration between Telegram and Europol has also resulted in strengthened content referral tools, whereby any user is able to refer content they deem inappropriate through the referral feature in groups and channels.[143]

France

Together with Germany, France has called on the European Commission to regulate encrypted messaging apps as a way to help tackle terrorism.[144] Specifically, Matthias Fekl, while he was French minister of the interior, requested that the police have the same level of access to online and technology operators as they have to demand information from telecommunications companies.[145]

As a result of pressure from France and Germany, the European Commission is proposing it alters the EU's ePrivacy Regulation, effectively allowing national government to sidestep specific privacy safeguards if national security is threatened – but that does not include regulating encryption.[146] The challenge facing national law enforcement agencies is the lack of legal tools to force technology companies to hand over encrypted data.[147] However, since the publication in January 2017 of the European Commission's proposals, negotiations at council level have stalled and remain so under the German presidency of the EU.[148]

---

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

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

142 *Ibid*.

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

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

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

146 *Ibid*.

147 *Ibid*.

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

In France, encryption providers are currently required to "enter into agreements with the government to facilitate access to data they encrypt or face fines".[149] In parallel, the prime minister's office has the power to "ban encryption services that fail to meet their legal obligations".[150]

Ghana

Since Ghana has very little experience of terror attacks – there have been only 21 incidents with 23 fatalities since 1970[151] – the Ghanaian government has not developed a robust governance framework for violent extremism online.[152]

Unlike Ghana, nearby West African neighbour Nigeria has struggled with major terrorist attacks for years. Groups such as Boko Haram and Islamic State West Africa Province have launched notorious attacks such as the kidnapping of female students in April 2014[153] and the January 2015 massacres, both in Borno state.[154] Boko Haram has begun to utilise social media platforms to produce propaganda and to recruit new members to its cause. The group mostly uses traditional social media platforms, such as Twitter, Facebook and YouTube, to post photos of soldiers, publicise beheadings and kidnappings, and spread anti-government messaging in an effort to recruit.[155] However, in recent years, Boko Haram has begun to use encrypted instant messaging apps such as Telegram to release propaganda material and denounce other groups.[156] In response to the growth of terrorism in the country, the Nigerian government in 2013 intensified its anti-terror laws and governance. As well as strengthening state counter-terrorism institutions, the government can now detain and prosecute terror suspects and issue the death penalty to those found to have committed or planning to commit a terrorist act.[157]

In terms of regulating Telegram and its alternatives, therefore, Ghana's regional neighbour has opted for a traditional, state-centric and top-down mode of governance. This form of governance centres around legislative measures, with less emphasis on cross-sector initiatives or engagement with civil society. Furthermore, state-centric governance has proved to result in unintended dangerous outcomes, for example government shutdowns of the internet or governmental use of social media to suppress political dissent.[158] Governments in Africa have exploited a legacy of violent colonial laws, historically used to violate freedoms against citizenry, to "legitimise many … attempts

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*. February 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. Accessed via: https://www.start.umd.edu/gtd/
152 See also: Policy Landscape section in previous GNET report, 'Artificial Intelligence and Countering Violent Extremism: A Primer'. Accessed via: https://gnet-research.org/wp-content/uploads/2020/09/GNET-Report-Artificial-Intelligence-and-Countering-Violent-Extremism-A-Primer.pdf
153 Mbah, F. (2019), 'Nigeria's Chibok schoolgirls: Five years on, 112 still missing,' Al Jazeera. Accessed via: 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.' Accessed via: https://www.amnesty.org.uk/nigeria-boko-haram-doron-baga-attacks-satellite-images-massacre
155 UN Development Programme and RAND (2018), 'Social Media in Africa.' Accessed via: https://www.africa.undp.org/content/rba/en/home/library/reports/social-media-in-africa-.html
156 Zenn, J. (2017), 'Electronic Jihad in Nigeria: How Boko Haram is Using Social Media,' *Terrorism Monitor*, vol. 15, no. 23. Accessed via: https://www.refworld.org/docid/5b728ca2a.html
157 'Nigeria: Extremism & Counter Extremism,' Counter-Extremism Project. Accessed via: 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. Accessed: https://law.yale.edu/isp/initiatives/wikimedia-initiative-intermediaries-and-information/wiii-blog/moderate-globally-impact-locally-content-moderation-particularly-hard-african-countries

to make extra-legal demands of the private sector."[159] Social media platforms and internet service providers have had to respond to extra-legal government shutdown demands, raising concerns about censorship and violating freedom of expression.[160]

Civil society groups and journalists have expressed concern around Ghana's future as regards to regulation of the internet and social media platforms.[161] For instance, the Ghanaian police chief announced a possible social media shutdown ahead of the country's 2016 elections (thankfully abortive).[162] Additionally, generous freedom of expression laws in Ghana leave digital spaces open to abuses, such as hate speech and cyberbullying (particularly of women).[163] Calls for tighter regulation of social media platforms, therefore, are growing.

In response to these calls, Ghana passed a Right to Information Bill in 2019, which guarantees access to information held by public institutions.[164] The Bill signals that the Ghanaian government wants to handle digital rights with transparency and accountability, and find a balance between protecting users from harm and protecting users' free speech. Nevertheless, the Ghanaian government could broaden its CVE strategy to engage and co-produce responses with civil society and community groups.

Japan

The Japanese government's counter-terrorism efforts are starkly divided between what it perceives as foreign and domestic terrorist activities. With this split institutional responsibility comes two different approaches to countering violent extremism online.

In terms of domestic threats, such as those posed by the Tokyo 2021 Olympic Games or the Japanese far right, the state response is largely coordinated by law enforcement agencies. Cold War-era communist subversion activities have influenced the way in which Japan handles domestic threats: prefectural police (overseen by the National Police Agency) and the Public Security Intelligence Agency (Japan's national intelligence agency) spearhead intelligence gathering and counter-terrorism efforts on Japanese soil.[165]

Domestic counter-terrorism activities, therefore, are centred around policing and traditional security architectures. Given its propensity for innovative technological developments, Japan has forged ahead with artificial intelligence-led solutions, including large-scale facial

159 Ilori, T. (2020), 'Stemming digital colonialism through reform of cybercrime laws in Africa,' Information Society Project at Yale Law School. Accessed: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.' Accessed: 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. Accessed: 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 August 2019. Accessed: 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. Accessed: 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 March 2019. Accessed: https://www.graphic.com.gh/news/politics/ghana-news-rti-bill-passed.html

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

recognition, biometric authentication and behaviour detection systems.[166] These solutions suggest a governance model centred around early detection and prevention, operationalised through traditional police and security tactics.

To shore up these efforts, Japanese Prime Minister Shinzo Abe pushed through[167] an anti-terror bill in mid-2017 described by Japan's opposition leader as "brutal."[168] The legislation criminalises planning to commit over 270 "serious crimes", including sit-in protests and music copyright infringements, and its enforcement extends to social media.[169] Civil rights activists and civil society groups are deeply concerned by the bill, given its broad remit and the power it grants to surveil and police online activity.[170]

As regards international counter-terrorism efforts, Japan's approach diverges from its domestic emphasis on criminalisation. Japan's overseas counter-terrorism efforts are regional, capacity-building and cooperative. More specifically, many of its CVE efforts form part of the Association of Southeast Asian Nations (ASEAN),[171] which issued a set of declaratory statements that commit signatories to "prevent, disrupt and combat international terrorism through information exchange, intelligence sharing and capacity building," establishing a precedent for regional cooperation to counter violent extremism and terrorism.[172]

Japan has twice hosted the annual ASEAN-Japan Counter Terrorism Dialogue, as well as engaging in bilateral talks with a range of global actors.[173] In late 2019, Japan and the UK held discussions on "the current situation of international terrorism, domestic measures to counter terrorism, and also on current counter-terrorism capacity building cooperation particularly in third [*sp.*] countries."[174]

Combatting extremists' use of Telegram and its alternatives in Japan is likely to follow this joint approach: an outward-facing strategy of regional cooperation and agenda-setting, with a domestic operationalisation based on traditional security, policing and surveillance activities.

166 The Government of Japan, 'All is Ready for a Safe and Secure Tokyo Games,' Autumn/Winter 2019. Accessed: 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. Accessed: https://www.nec.com/en/press/201502/global_20150219_01.html; Kyodo News, 'Kanagawa police eye AI-assisted predictive policing before Olympics,' 29 January 2018. Accessed via: https://english.kyodonews.net/news/2018/01/5890d824baaf-kanagawa-police-eye-ai-assisted-predictive-policing-before-olympics.html

167 The Bill passed via "the unusual step of skipping a vote in the Upper House Committee on Judicial Affairs." Japan Federation of Bar Associations, 'Statement on the Enactment of the Bill to Revise the Act on Punishment of Organized Crimes and Control of Crime Proceeds, including the Criminalization of Conspiracy,' 15 June 2017. Accessed via: 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 June 2017. Accessed via: https://foreignpolicy.com/2017/06/16/japan-just-passed-a-brutal-defective-anti-terror-law/

169 McCurry, J., 'Japan passes "brutal" counter-terror law despite fears over civil liberties,' *The Guardian*, 15 June 2017. Accessed via: 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 June 2017. Accessed via: http://www.thedailybeast.com/japans-terrible-anti-terror-law-just-made-the-minority-report-reality

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

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

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

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

174 Ministry of Foreign Affairs of Japan, 'The 4th Japan-the UK Counter-Terrorism Dialogue,' 4 December 2019. Accessed via: https://www.mofa.go.jp/fp/is_sc/page1e_000297.html

New Zealand

Released in February 2020, New Zealand's overarching counter-terrorism strategy shows that governance of countering violent extremism online involves the coordination of manifold agencies and bodies.[175] Similar to Canada (above), these bodies range from the Cabinet External Relations and Security Committee to police, intelligence and security communications agencies, as well as foreign affairs, trade, defence, transport, innovation and development agencies.

New Zealand has garnered international attention for its leadership in cross-country and cross-sector initiatives. Most notably, in the aftermath of the Christchurch mosque shootings in March 2019, the governments of New Zealand and France brought together a coalition of heads of state with social media and technology companies under the Christchurch Call to Eliminate Terrorist and Violence Extremist Content Online.[176] Signatories to the call are committed to enforce laws that prohibit the dissemination of terrorist and violent extremist content online, yet also respect freedom of expression and privacy concerns. The countries also work to support frameworks, capacity-building and awareness-raising activities in order to prevent the use of online services to disseminate terrorist and violent extremist content.

The Christchurch Call also commits companies, including Amazon, Facebook, Google, Twitter, Facebook and YouTube, to greater industry standards of accountability and transparency. The companies must enforce their community standards and terms of services by prioritising content moderation and removal actions, and identifying content in real-time for review and assessment. Collectively, the countries and companies are developing efforts with civil society to promote community-led activities in order to intervene in the processes of online radicalisation.

The call also acted as the vehicle through which the GIFCT was overhauled. As part of the overhaul, GIFCT's remit expanded to include a suite of preventative, response and educational activities in the effort to counter violent extremism online.[177]

New Zealand's efforts to co-sponsor a range of cross-sector global initiatives showcase a more horizontal approach to governing extremists' use of tech platforms. The approach encompasses conventional security and intelligence structures as well as initiatives that bring together practitioners, academia, policymakers and tech leaders to formulate responses to emerging violent extremist threats online.

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

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

177 Global Internet Forum to Counter Terrorism, 'Next Steps for GIFCT,' 23 September 2019. Accessed via: https://gifct.org/press/next-steps-gifct/

United Kingdom

The United Kingdom's approach to combating extremist use of online platforms follows a traditional mode of governance that centres on state institutions. The central institution responsible for counter-terrorism legislation is the Home Office, which also coordinates with the Government Communications Headquarters, the country's security and intelligence organisation. The Home Office has also created collaborative bodies with other government institutions (most often the Department for Digital, Culture, Media, and Sport) and Parliament, such as the UK Council for Internet Safety, the National Counter Terrorism Security Office and the Commission on Countering Extremism.[178]

Similar to Japan's (above), the UK has a two-pronged approach to countering violent extremism online. The first track of activity is centred around regulation of social media and technology platforms. The government's Online Harms White Paper, published in April 2019, set out a comprehensive case for greater national regulation of social media.[179] Under this new regulatory framework, social media and technology companies will bear a new statutory duty of care to their users, enforceable via Ofcom, the UK's regulatory body for communications. Ofcom will subject platforms to financial and technical penalties – websites could be blocked at ISP level and fined up to 4% of their global turnover – for non-compliance with the framework and violations of the statutory duty of care.[180] At the time of writing, the Online Harms Bill, the legislative operationalisation of the White Paper, has been delayed for several years.[181]

The second approach pursued by the UK is focused on conventional policing, security and intelligence institutions, buttressed by counter-terrorism legislation and strong public support. In Spring 2020, Parliament introduced new proposed counter-terrorism legislation that targets suspects of terrorist activities. Under the new legislation, suspects "who have not been convicted of any offense could potentially face expanded and increased surveillance measures."[182] These surveillance measures would no longer be subject to a two-year cap. Additionally, terrorism prevention and investigation measures (known as Tpims), including mandatory relocation, electronic monitoring tagging, exclusion from specific places and limits on travel, association, financial services and the use of communications, will now be easier to impose under the proposed reduced burden of proof.[183]

These stricter counter-terrorism measures come after attacks at Fishmongers' Hall in the City of London in November 2019 and on Streatham High Road in February 2020,[184] as public opinion supported

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

179 HM Government, 'Online Harms White Paper,' April 2019. Accessed: 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 June 2020. Accessed: https://www.bbc.co.uk/news/technology-53222665

181 *Ibid*.

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

183 Grierson, J., 'Unconvicted terrorism suspects face indefinite controls under UK bill,' *The Guardian*, 20 May 2020. Accessed via: https://www.theguardian.com/politics/2020/may/20/unconvicted-terrorism-suspects-face-indefinite-controls-under-uk-bill

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

tougher legislation.[185] Given this permissive zeitgeist, approaches to countering violent extremism online, particularly the use of applications such as Telegram and its alternatives, may turn away from a regulatory approach and towards a law enforcement one. Under the proposed bill, the burden of proof for subjecting a citizen to Tpims will be reduced to "reasonable grounds."[186] It remains unclear whether the use of applications such as Telegram and other decentralised and encrypted text-based instant messaging applications to access or spread extremist content will count towards such reasonable grounds.

UN Counter-Terrorism Committee Executive Directorate

The UN General Assembly unanimously adopted the United Nations Global Counter-Terrorism Strategy in 2006. Since then, the Security Council has adopted a number of resolutions focused on tackling terrorism that require Member States to fully cooperate in the fight against terrorism. Resolutions 1373 (2001) and 1566 (2004) "require legislative action to be taken by all Member States to combat terrorism, including through increased cooperation with other governments."[187] Resolution 1963 (2010) recognises the increased use of the internet by terrorists for terrorist purposes.[188]

Tackling terrorist organisations' use of decentralised platforms poses challenges for law enforcement agencies. These platforms do not require any intermediary to send and receive messages, making the tracking of (suspected) terrorists very difficult.[189]

The UN has called for national governments to provide a "clear legal basis for the obligations on private sector parties" under which technology companies and platforms should cooperate with law enforcement authorities during investigations.[190]

United States

The USA's policy approach to combating the misuse of tech platforms can be described as irregular. In terms of state institutions involved, the Department of Homeland Security (DHS), the Department of Justice, the Federal Bureau of Investigation, the National Counter Terrorism Center, the National Security Council and Congress, among others, are at the forefront of the response.[191] A range of methods have been tried: "counter messaging, awareness briefings, partnerships, and legislation."[192]

185 In a September 2017 report that included polling on attitudes towards extremist content online, nearly three-quarters of responded would support new legislation criminalising the possession and consumption of extremist content online. See: Frampton, M. (2017), 'The New Netwar: Countering Extremism Online,' *Policy Exchange*. Accessed via: 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,' June 2020. Accessed via: https://publications.parliament.uk/pa/cm5801/cmpublic/CounterTerrorism/memo/CTSB07.pdf

187 UNODC, *The use of the Internet for terrorist purposes*. United Nations, 2012. p. 16 https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

188 *Ibid*.

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

190 UNODC, 2012. p. 135

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. Accessed via: https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/A%20Plan%20for%20Preventing%20and%20Countering%20Terrorist%20and%20Violent%20Extremist.pdf

192 *Ibid*.

One such method was co-sponsorship of global cross-sector initiatives. The USA's Counter-Terrorism Strategy commits itself to working with business and industry to combat terrorist recruitment, fundraising and radicalisation processes online. In terms of cross-country initiatives, the USA works with initiatives such as Tech Against Terrorism and the Global Counterterrorism Forum, which relies on partnership with other signatories, civil society and the tech sector to craft medium- and long-term approaches to countering violent extremism online.

More broadly, the Obama administration launched the Countering Violent Extremism Task Force in 2011, in order to "unify the domestic CVE effort."[193] The Task Force is intended to bring together practitioners from the bodies listed above in order to coordinate engagement with civil society, develop intervention models, invest in research and cultivate communications and digital strategies.[194] Given the USA's previous sporadic efforts, a unified approach to countering violent extremism online would bolster efforts to combat the misuse of platforms such as Telegram.

However, in early 2017, President Trump considered restructuring the Task Force to remove white supremacist terrorism from its remit, renaming the programme the 'Countering Radical Islamic Extremism.'[195] Furthermore, a budget unveiled in Spring 2017 cut all funding to countering violent extremism programmes.[196] By late October 2018, the Task Force had shuttered: funding expired and "staff members returned to their home agencies and departments."[197]

Trump's actions reveal a deep hostility towards CVE efforts generally, but specifically those aimed at community outreach and engagement with local civil society and those targeting far-right and white supremacist terrorism. For instance, one of the recipients of DHS funding was Life After Hate, an initiative that works with individuals to help them to leave white supremacist and neo-Nazi groups.[198] Removing funding and curtailing remit to exclude white supremacy from the USA's efforts can be understood as a flagrant signal that the Trump administration will not act against white supremacist and racist terrorist actions.

This development has grave significance for combating the use of Telegram and other encrypted and decentralised instant messaging applications. As Bennett Clifford shows above, many of these platforms are utilised by far-right groups to coordinate activities. If governmental responses to these platforms is proven to now be "politically motivated and dangerous,"[199] we can reasonably look upon the future of CVE with worry. The final line of defence against exploitation of these platforms will be increased pressure upon their founders to comply with law enforcement and court orders, an approach that will surely prove to be too little, too late.

193 Department of Homeland Security, 'Countering Violent Extremism Task Force.' Accessed via: 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 February 2017. Accessed via: 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 May 2017. Accessed via: https://www.reuters.com/article/us-usa-budget-extremism-idUSKBN18J2HJ

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

198 Life After Hate, 'About Us.' Accessed via: 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 February 2017. Accessed via: https://www.splcenter.org/news/2017/02/02/splc-trumps-planned-changes-governments-countering-violent-extremism-program-are

Towards a Decentralised Mode of Governance for Decentralised Platforms?

In the report above, Bennett Clifford warns of the increasing move that Telegram-like applications are making towards decentralised server-hosting. This feature, emerging with the advent of Web 2.0, would allow users to communicate directly with one another, bypassing centralised services provided by corporations such as Google, Amazon, Microsoft and Facebook.[200] The decentralised model "reverses the current data ownership model," so that users will have full access and ownership over their own data.[201]

Government-owned centralised service provision provides ample opportunity for abuse, surveillance and censorship. For instance, the Indian government imposed the world's longest internet shutdown in Kashmir as part of India's decades-long anti-Muslim violence and atrocities.[202] The shutdown, lasting 192 days, is part of a broader, worrying attitude towards digital rights in India: the communications and information technology minister has questioned citizens' right to the internet, announcing that "While right of internet is important, security of the country is equally important … Can we deny [that] the internet is abused by terrorists?"[203]

Similarly, corporations have been known to misuse users' data. In 2018, political consulting firm Cambridge Analytica harvested millions of Facebook users' personal data for political advertising.[204] The data breach, the largest in Facebook's history, was utilised by presidential candidate Donald Trump in 2016 in order to micro-target Facebook users identified as swing voters.[205] Since users' data is centralised on Facebook servers, the platform can monetise, surveil and misuse billions of peoples' sensitive and personal information.[206]

A decentralised internet model, while safeguarding data by keeping it out of reach, also poses its own challenges. In particular, decentralised and encrypted instant messaging apps, including Telegram and its alternatives, can provide a safe haven for extremist content. As Clifford writes above, a decentralised server-hosting feature on emerging platforms "will inevitably make these platforms more accessible to extremist groups." A decentralised platform can far more easily evade surveillance and intervention from both self-regulating platforms and law enforcement orders, since data will no longer be in their hands.

Combating the exploitation and misuse of decentralised instant messaging platforms raises urgent and challenging questions around

200 Corbyn, Z. 'Decentralisation: The Next Big Step for the World Wide Web,' *The Guardian*, 8 September 2018. Accessed via: 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 December 2018. Accessed via: 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 December 2019. Accessed via: https://www.opendemocracy.net/en/openindia/india-escalating-kashmir-conflict-painting-it-terrorism/

203 Shastry, V. 'Asia's Internet Shutdowns Threaten the Right to Digital Access,' *Chatham House*, 18 February 2020. Accessed via: 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 April 2018. Accessed via: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

205 Hilder, P. and Lewis, P. 'Leaked: Cambridge Analytica's Blueprint for Trump's Victory,' *The Guardian*, 23 March 2018. Accessed via: 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 February 2019. Accessed via: https://palladiummag.com/2019/02/14/facebooks-political-problems-are-inherent-to-centralized-social-media/

governance. How should governments and corporations respond to extremist use of a decentralised internet? How can users' rights to privacy and freedom of expression be balanced against users' exploitation of platforms to spread propaganda and misinformation, recruit to their causes and plan terrorist attacks?

Within current modes of governance, there are three possible routes, each broadly tied to a stage along a linear radicalisation process.

The first approach – early prevention – aims to intervene in the early stages of radicalisation to stop people from engaging with terrorist content. In terms of Telegram-like applications, an early prevention approach would work to prevent people from seeking to engage with extremist content, groups and channels on the platform. The benefit of this approach is that it mitigates resource-heavy policing of the platform and weakens the online presence of extremists while keeping users' freedom of expression and privacy rights intact.

However, early prevention programmes are themselves mired in other ethical, political and legal challenges. Perhaps the most notorious early prevention programme is the UK Home Office's Prevent Strategy, introduced in 2003. The strategy targets "individuals who are vulnerable to recruitment", particularly within institutions such as the NHS, schools, universities and other local communities and civil society groups.[207] Prevent has been criticised since its inception by civil liberties groups: Shami Chakrabarti, then-Director of Liberty, a prominent civil rights group, named Prevent as "the biggest spying programme in Britain in modern times", since the intelligence gathered on so-called vulnerable individuals includes political and religious views, mental health information and sexual activity.[208] Prevent overwhelmingly targets British Muslims, shoring up Islamophobia and conflating "legitimate political resistance among young British Muslims" with "indications of violent extremism".[209]

The second mode of governance focuses on disengagement and counter-messaging. Individuals who are already accessing and consuming extremist content online can be targeted with counter-narratives to offer "credible alternative interpretations of the world and directions for agency and action to those being circulated by violent extremist groups" through the reaffirmation of tolerance, openness, freedom and democracy.[210] For instant messaging platforms like Telegram, this could involve the infiltration of channels and groups to post alternative narratives in the hopes of diverting some individuals away from radicalisation.

Counter-messaging has potential, but government-led strategic communications have been largely ineffective,[211] and had negative unintended consequences. The US Department of State's Think

207 UK Home Office, 'Counter-Terrorism Strategy: The Four Ps: Pursue, Prevent, Protect, Prepare'. Accessed via: https://web.archive.org/web/20090711105017/http://security.homeoffice.gov.uk/counter-terrorism-strategy/about-the-strategy1/four-ps/; HM Government, 'CONTEST: The United Kingdom's Strategy for Countering Terrorism,' June 2018. Accessed via: 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 October 2009. Accessed via: https://www.theguardian.com/uk/2009/oct/16/anti-terrorism-strategy-spies-innocents

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

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

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

Again Turn Away programme, which disseminated counter-messaging material and engaged in disputes on Twitter with IS and pro-IS accounts produced backlash and ire.[212] Research undertaken by Demos found that European counter-speech pages on Facebook attracted low levels of overall engagement.[213] Government-backed strategic communication initiatives lack credibility due to the so-called "say-do" gap, whereby the violent extremist message is reinforced through the presentation of the gap between the values governments promote and their actions.[214]

As a consequence, subsequent efforts at counter-messaging initiatives online often de-emphasise governmental involvement and are led by industry. Google and its parent company, Alphabet, have pioneered the use of the "content redirect method", which targets individuals browsing IS content online and redirects them to curated videos on YouTube that counter VE messaging.[215] The curated video content exposes vulnerable and radicalised individuals to narratives that emphasise values such as tolerance, diversity and inclusivity. Alphabet's flagship partner for the content redirect method is Moonshot CVE, which runs counter-messaging campaigns in over twenty-eight countries in fifteen languages.[216] The US-based Anti-Defamation League has teamed up with Moonshot CVE to counter white supremacist and jihadist activity online.[217]

While Moonshot CVE's efforts have potential to disrupt the radicalisation journey, industry-led solutions to deep sociopolitical problems have their own challenges. Moonshot CVE, as an independent company, is beyond the reach of government or civil society oversight or accountability. The company discloses only high-level data as regards its operations and it is not clear how and why the redirected is selected.[218]

The third mode of governance – regulation of platforms – comes towards the end of the radicalisation process. In the report above, Clifford describes the efforts by law enforcement to pressurise platforms such as Telegram to comply with court orders for suspected terrorist activity. For instance, on page 5, Clifford described the Europol referral action days, which successfully resulted in Telegram updating its privacy policy to include a clause which states that the platform may share user data with the authorities for identification purposes in cases of suspected extremist content. Other platforms detailed in the report above have collaborated to greater and lesser extents with governments and law enforcement agencies to combat the proliferation of extremist content.

The challenge in this mode of governance is that policymakers and law enforcement agencies are engaged in 'whack-a-mole' regulatory efforts: once a platform agrees to collaborate with court orders, another alternative platform springs up in its place to offer safeguarded

212 Katz, R. (2014) 'The State Department's Twitter War with ISIS is Embarrassing,' *Time*. Accessed: https://time.com/3387065/isis-twitter-war-state-department/
213 Bartlett & Krasodomski-Jones, 'Counter-Speech'
214 Romaniuk, P. (2015) 'Does CVE Work? Lessons Learned from the Global Effort to Counter Violent Extremism,' *Global Center on Cooperative Security*. Accessed: https://www.globalcenter.org/wp-content/uploads/2015/09/Does-CVE-Work_2015.pdf, p.33
215 See: https://redirectmethod.org/
216 See: http://moonshotcve.com/work/
217 'ADL and Partners Counter White Supremacists Online Through Google Search,' *Anti-Defamation League*. Accessed: https://www.adl.org/news/press-releases/adl-and-partners-counter-white-supremacists-online-through-google-search
218 See: http://moonshotcve.com/work/

privacy to users. As the report above concludes, "With the emergence of increasingly stable instant messaging platforms offering new privacy and security features, extremists making the jump from Telegram to a secondary instant messenger raises questions of 'when' and 'which', not 'if'."

A features-centric approach to combating online extremism, as outlined in the final pages of the report above, opens up the possibility of a new form of governance beyond the three approaches described here. Each of the modes above relies upon vertical, top-down governance, often via state institutions resting upon legislative justification.[219] Early prevention, counter-messaging and regulation each subscribe to a 'command-and-control' governance structure in which entities (governments, corporations, law enforcement agencies, intelligence agencies) create and direct policy downwards.

A decentralised web, defined by the features it offers to users, could necessitate a more decentralised mode of governance. In place of a vertical governance structure, a horizontal approach to policymaking that mimics the structure of a decentralised internet could be effective. Cross-sector initiatives, such as an expanded GIFCT as Clifford describes on page 26 above, which brings together a wider suite of service providers along with policymakers and academic experts, is a good example of a more decentralised approach.

A previous report by GNET, *Artificial Intelligence and Countering Violent Extremism,* recommended that an independent regulatory body could be highly effective in moderating harmful content online.[220] Co-regulation between civil society, government, industry and service providers, overseen by a cross-national and independent body, enshrines a more horizontal and inclusive mode of CVE governance. This body could indeed be structured around features of decentralised platforms and violent extremist content online, as Clifford suggests above, in order to "proactively prepare responses … [and] disrupt the process of extremist adoption of new platforms." Such a decentralised mode of governance could provide to be highly effective in adapting to and meeting the challenges of a shift towards a decentralised internet.

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

220 GNET, 'Artificial Intelligence and Countering Violent Extremism: A Primer', p. 41. Accessed via: https://gnet-research.org/wp-content/uploads/2020/09/GNET-Report-Artificial-Intelligence-and-Countering-Violent-Extremism-A-Primer.pdf

Global Network
on Extremism & Technology

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

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

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.