IDC HERZLIYA
ICT International Institute for Counter-Terrorism
With the Support of the Jusidman Foundation

Hiding to Fight Another Day:
Far-Right Extremists Adopt a New Strategy in the Cyberspace Arena after 6 January Capitol Attack

Dr. Liram Koblentz-Stenzler, Alexander Pack

June 2021

Synopsis

6 June marked five months since the U.S. Capitol was attacked. Posts regularly collected from far-right communication channels during that time suggests that there has been a significant shift in the far-right's strategic behavior within cyberspace. In an effort to support the Biden Administration's "first ever national strategy for countering domestic terrorism," the purpose of this paper is to help decision-makers and security forces understand this developing phenomenon within the American far-right online community.[1] Routine monitoring of encrypted and unencrypted far-right communication channels indicates that due to their fear of increased scrutiny following the events of 6 January, members of the far-right have attempted to consolidate their security and increase the difficulty of tracking their communications.

This article will demonstrate how immediately after the 6 January attacks, far-right users on multiple sites became concerned about the potential for being tracked online or removed from various platforms. In response to this fear, members of the far-right began engaging in a simultaneous defensive and offensive strategy. Defensively, far-right actors worked to secure existing lines of communication while locating and migrating to more secure communication platforms. Concurrently, they also began implementing an offensive strategy to counter potential investigators by doxing specific individuals while organizing "mass reporting" campaigns to de-platform others.

Although these changes in strategy, at first, appeared to only be in response to the increased scrutiny from the Capitol attack, their continued use suggests that they may be a permanent or semi-permanent shift in the broader far-right strategy in cyberspace. Security forces and decision-makers in the United States must recognize this shift and implement new methods to monitor far-right actors online. Failing to respond to this significant change may allow extremist actors to plan, organize, and execute future attacks undetected.

Introduction

Like other criminal or illicit organizations and movements, American far-right extremists have often tried "to keep their activities secret" in order to remain hidden from law enforcement, journalists, and the public.[2] After attacks, these same movements or organizations are often exposed to increasing levels of scrutiny and may attempt to "lay low" to avoid detection and thus potentially arrest. The actions of the American militia movement following the 1995 attack in Oklahoma City serve as a prime example.

[1] David Smith, "White House Unveils First National Strategy to Fight Domestic Terrorism," The Guardian (Guardian News and Media, June 15, 2021), https://www.theguardian.com/us-news/2021/jun/15/white-house-domestic-terrorism-plan-biden.

[2] Matteo Gregori and Ugo Merlone, "Comparing Operational Terrorist Networks," *Trends in Organized Crime* 23, no. 3 (March 31, 2020): pp. 263-288, https://doi.org/10.1007/s12117-020-09381-z, 264.

In 1995, partially inspired by the American militia movement, Timothy McVeigh executed a bombing attack against the Alfred P. Murrah Federal Building in Oklahoma City, ultimately causing the death of 168 people and injury to more than 700 more.[3] Although not directly responsible for the attack, "the public, media, and law enforcement" exercised increased scrutiny over the militia movement.[4] As a result of this increased negative attention, the militia movement was "placed on the defensive."[5] Hoping to avoid potential arrests or investigations, many militia groups at the time attempted to "scale back, distance themselves from McVeigh" and his actions.[6] According to some scholars, this increased negative attention combined with mass arrests and the economic stability in the United States resulted in the militia movement remaining relatively hidden until 2008.

Routine monitoring of far-right communications suggests that the 6 January attack has inspired similar behavior among the American far-right today. Posts and other communications collected indicate that because of their concern regarding increasing scrutiny following the Capitol attack, members of the far-right have attempted to consolidate their security and increase the difficulty of tracking their communications. This paper will explore concerns expressed by far-right actors: (i) fear that they are being tracked online, (ii) fear that they are being removed from cyberspace; Additionally, this paper will examine a potential new strategy they have deployed to avoid exposure or de-platforming: (i) securing existing communication platforms, (ii) migrating to more secure communication platforms, (iii) countering potential investigators.

Reason to Hide

Like the Oklahoma City bombing executed by Timothy McVeigh in 1995, the 6 January attack has drawn increasingly negative attention to the motivations, organizations, and actions of the American far-right. Given this increased negative attention, far-right individuals, organizations, and platforms have received ever-increasing scrutiny from law enforcement, journalists, and individual actors. Just as the militia movement attempted to after the Oklahoma City bombing, current far-right actors have responded to this increased scrutiny by retreating "underground" in an effort to avoid detection. Based on monitoring of clear- and darknet platforms, it appears that far-right actors have shown an increased interest in exercising discretion for two primary reasons: (i) fear that they are being tracked online, (ii) fear that they are being removed from the cyberspace.

---

[3] Kelly-Leigh Cooper, "Oklahoma City Bombing: The Day Domestic Terror Shook America," BBC News (BBC, April 19, 2020), https://www.bbc.com/news/world-us-canada-51735115.

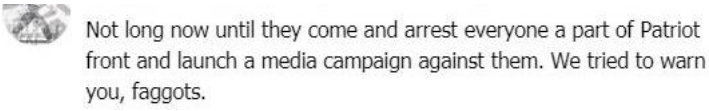
[4] Arie Perliger, *American Zealots: inside Right-Wing Domestic Terrorism* (New York City, New York: Columbia University Press, 2020), 57.

[5] Ibid.

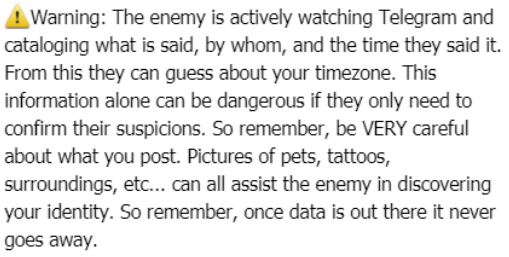
[6] Richard Leiby, "Many Militia Groups Scale Back, Distance Themselves From McVeigh," The Washington Post (WP Company, June 14, 1997), https://www.washingtonpost.com/wp-srv/national/longterm/oklahoma/stories/militia.htm.

i. Fear the Far-Right is Being Tracked Online

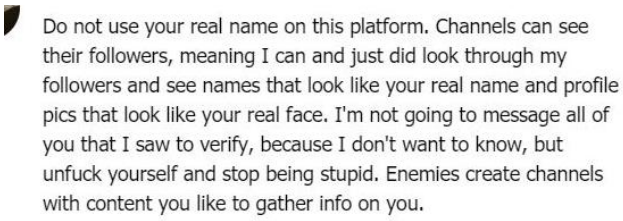
In the days following the 6 January attack, local and national law enforcement agencies began a concerted effort to locate and arrest any individuals who planned, participated, or assisted in the storming of the Capitol.[7] Noticing this increased interest, far-right extremists began sharing posts suggesting that federal law enforcement was monitoring all far-right actors online and in the real world. Ultimately, the far-right actors began to fear that law enforcement officials would execute mass arrests based on any information gathered.



Post suggesting that federal law enforcement would soon "arrest everyone" involved in the movement (Telegram, 11 January 2021)



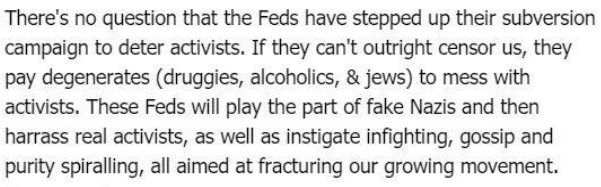
Telegram post suggesting that investigators are "actively watching" far-right Telegram channels in an effort to identify individuals (Telegram, 12 January 2021)



Post shared shortly after the attack at the Capitol, which suggested that "enemies" were attempting to gather intelligence on far-right actors; ultimately, the user encourages better "OPSEC" (Telegram, 14 January 2021)

While routine monitoring of far-right communications suggested that far-right actors have always expressed some concern regarding the potential for infiltration, their concerns were intensified after the 6 January attack. For instance, while actors regularly shared content referencing online security and "OPSEC" before the storming of the Capitol, after the attack, the volume of posts appeared to triple.[8] This was likely in response to their belief that "the Feds have stepped up their subversion campaign" following 6 January.

[7] Josh Gerstein, "FBI Arrests Man Who Posted Photo of Himself with Feet up in Pelosi's Office," POLITICO (POLITICO, January 10, 2021), https://www.politico.com/news/2021/01/08/fbi-arrest-rioter-pelosi-office-456580.
[8] In the far-right lexicon, "OPSEC" or "opsec" is a reference to broad "operational security" guidelines that online users should utilize to avoid detection by investigators.

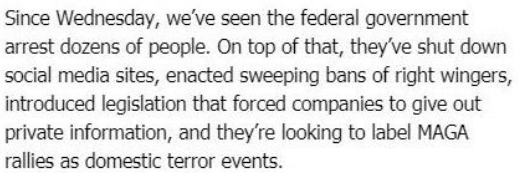


Telegram post suggesting that federal law enforcement officials are attempting to subvert the actions of far-right actors (Telegram, 5 February 2021)

Although initially restricted to far-right Telegram channels, fear of law enforcement infiltration and arrests also spread to other sections of the far-right online ecosystem, specifically to militia-focused discussion boards. For example, on one unencrypted message board, users stated that they were "visited" by federal agents who were "conducting investigations" into social media posts by "conservatie and libertarian citizens" [sic] following the 6 January attack on the U.S. Capitol. While the authors were not able to, or chose not to, substantiate these claims when questioned, many users stated they believed such investigations were imminent.

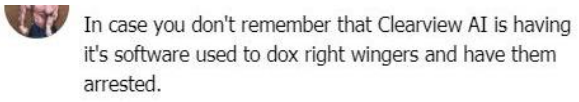
Post claiming that agents from the FBI are targeting "CONSERVATIE AND LIBERTARIAN CITIZENS" [sic] after the attack at the Capitol building (Militia Message Board, 17 January 2021)

In addition to general monitoring by law enforcement, users also began to fear the potential of local and federal agencies partnering with high-tech companies to identify and arrest far-right actors. Specifically, users discussed their belief that the federal government was monitoring and "shut[ing] down social media sites" predominantly used by far-right supporters. Similarly, far-right actors began to express concern regarding the use of "Clearview AI" to "dox right wingers and have them arrested" [sic].[9]



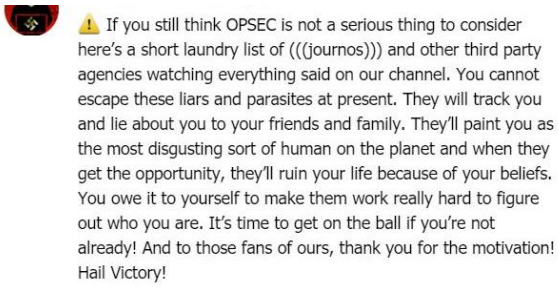
Telegram post arguing that law enforcement is attempting to gather information on far-right actors from social media companies (Telegram, 15 January 2021)

[9] Clearview AI is a technology start-up that has developed a proprietary facial recognition system using images scraped from the internet. The company then utilizes artificial intelligence algorithms to to identify individuals. For more information on Clearview AI, see: Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," The New York Times (The New York Times, January 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

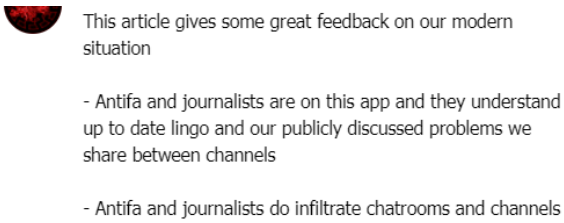


Post claiming that law enforcement officers are utilizing an advanced artificial intelligence software to "dox right wingers and have them arrested" (Telegram, 27 January 2021)

While continuing to express the concern of being identified by law enforcement agencies, far-right actors also began to fear the potential of journalists monitoring their communications and online activity. For example, multiple unencrypted far-right Telegram channels and encrypted darknet forums began to distribute "a short laundry list of (((journos))) and other third party agencies" monitoring far-right platforms following the 6 January attack.[10] Users suggested that these journalists would continue tracking the far-right for the foreseeable future, and as such, it was necessary to improve their "OPSEC."

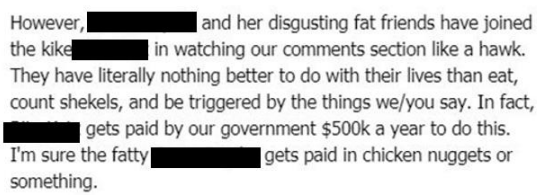


Telegram post suggesting that followers of far-right channels are being targeted by journalists and other independent agencies (Telegram, 2 February 2021)



Post suggesting that "Antifa and journalists do infiltrate" and monitor far-right communications online (Telegram, 10 April 2021)

In addition to circulating general lists of publications and agencies monitoring the far-right online, far-right users also attempted to identify individual journalists and alleged members of "Antifa" whom they believed were gathering information by "watching [far-right] comments sections like a hawk."[11]



[10] In the far-right lexicon, the use of three parentheses surrounding a word or name is often referred to as the "echo." This "echo" is used to indicate to other far-right actors that the individual, group, or information contained within the "echo" is Jewish. For further reading on the use of the "echo" by the far-right, see: "Echo," Anti-Defamation League, accessed June 5, 2021, https://www.adl.org/education/references/hate-symbols/echo.

[11] This journalists names have been omitted for their privacy.

Post suggesting that journalists (whose names have been omitted) are monitoring far-right channels "like a hawk" to report them[12] (Telegram, 26 January 2021)

Similar to journalists, far-right actors also began to fear the potential of being monitored or exposed by individual actors. For example, several users discussed a privately owned website that was attempting to identify any far-right actors who had participated in the attack on the U.S. Capitol.

Post highlighting a "privately owned website" that is attempting to identify far-right actors who participated in the 6 January attack. Far-right actors claim that this is because "they want [the far-right] dead" (Telegram, 9 January 2021)

ii. Belief They Are Being "Purged" or Removed from Cyberspace

On 8 January 2021, just two days after the attack on the U.S. Capitol, Twitter formally suspended former President Trump's official Twitter account, @realDonaldTrump.[13] Citing concerns over the potential for violence, Twitter barred the former president from utilizing his @realDonaldTrump account or any other account, such as @POTUS.[14] In the following weeks, multiple major social media companies increased their efforts to remove extremist content, with Twitter suspending "more than 70,000 accounts associated with the far right QAnon conspiracy."[15] In parallel, Facebook took an aggressive stance by indefinitely barring former President Trump from posting on the platform while also removing posts supporting the unsubstantiated theory that the 2020 election was fraudulent.[16]

---

[12] In the lexicon of the far-right, "kike" is a derogatory term referencing someone of Jewish descent.
[13] Brian Fung, "Twitter Bans President Trump Permanently," CNN (Cable News Network, January 9, 2021), https://www.cnn.com/2021/01/08/tech/trump-twitter-ban/index.html.
[14] Ibid.
[15] "Social Media Crackdown Continues After Siege of US Capitol," U.S. News & World Report (U.S. News & World Report, January 12, 2021), https://www.usnews.com/news/politics/articles/2021-01-12/social-media-crackdown-continues-after-siege-of-us-capitol.
[16] Sarah E. Needleman, "Facebook Says It Is Removing All Content Mentioning 'Stop the Steal'," The Wall Street Journal (Dow Jones & Company, January 12, 2021), https://www.wsj.com/articles/facebook-says-it-is-removing-all-content-mentioning-stop-the-steal-11610401305?reflink=share_mobilewebshare.

Noting the rise in de-platforming and content moderation, far-right actors began to express fear that they would be "purged" from the internet after the 6 January attack. Specifically, users suggested that given recent events, far-right channels may be "more susceptible to mass reporting" and thus de-platforming.

> **EXPECT THIS TO HAPPEN MORE FREQUENTLY TO ALL OF US**
>
> **25 MILLION POLITICALLY LOST INDIVIDUALS HAVE ENTERED OUR DOMAIN WITHIN THE LAST FEW DAYS**
>
> **ON TOP OF THIS MASSIVE ATTENTION HAS BEEN BROUGHT TO OUR LAST BASTION OF FREE SPEECH, MAKING TERRORGRAM MORE SUSCEPTIBLE TO MASS REPORTING**

Post suggesting that far-right channels in "TERRORGRAM" may be susceptible to de-platforming efforts given the increased attention after the 6 January attacks[17] (Telegram, 12 January 2021)

Multiple users expressed fear of being "shoa'd" or "shoahed" from the internet. In the far-right lexicon, "shoa'd" is an anti-Semitic phrase meaning to be destroyed. It refers to the Hebrew word "Shoah," which is one of the most common terms used to describe the Holocaust. Far-right actors often use the term as a way to mock both Jewish individuals in general and the Holocaust in particular.

> Due to the recent purges of our people from (((social media))) platforms we would like to inform the newcomers and remind those who have been around for a while that we still have our hidden service on the Tor network. In case of a Shoah in Telegram you will always be able to find us there. If something happens to this channel we have a backup channel @privsecbackup and we also have several archives of our posts.

Post highlighting the increasing "purges of [their] people" from social networking platforms following the event at the Capitol building (Telegram, 10 January 2021)

As Telegram began shutting down channels that violated the companies terms of service in mid-January, the concerns of far-right actors again increased. As more users were barred from the platform, multiple channels suggested that they were actively seeking alternative lines of communication to utilize if they were also removed.

> That said, we know far too well that our time here is short. The enemy knows our message of truth is incompatible with the anti-White System, and are doing everything in their power to divide and conquer us. Our channel in particular has empowered an incalculable number of dissidents on and off Telegram.
>
> We are working on alternative communication methods, but it appears several large channels are getting removed by Telegram as I type this. If we go dark before the big one, just know that whether you've been with us since the start, or are just finding us now, it has been an honor to share our time and knowledge with you.

[17] In the lexicon of the far-right "Terrorgram" is a portmanteau of the words "terror" and "Telegram;" it is a term used to describe channels on Telegram that promote far-right extremist ideologies such as accelerationism.

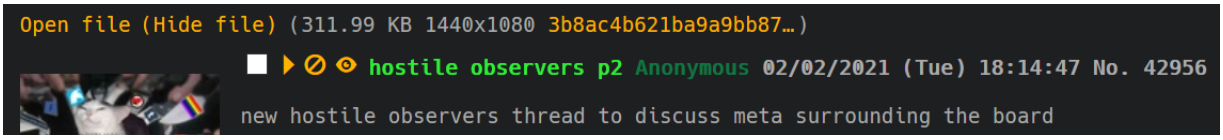
Telegram post explaining their belief that several prominent far-right channels were removed by Telegram, with the users expressing concern that their channel could be removed as well (Telegram, 12 January 2021)

Actions Taken to Hide

Fearing the potential of being exposed and arrested or removed from the cyberspace, as was emphasized in the posts above, far-right extremists appeared to take a defensive posture online. Routine monitoring of far-right communications detected three primary methods that the far-right is attempting to utilize in order to avoid exposure or de-platforming: (i) securing existing communication platforms, (ii) migrating to more secure communication platforms, (iii) countering potential investigators.

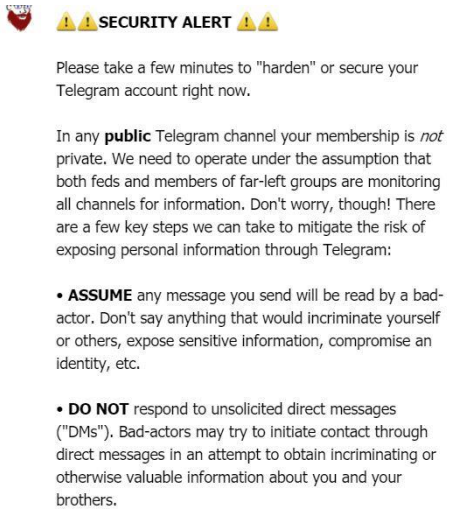
i. Securing Existing Platforms

Immediately after the 6 January attack and subsequent increased scrutiny, many far-right extremists began to discuss the inherent vulnerabilities in their current communication platforms. Specifically, several users discussed the ease with which "hostile observers" could infiltrate their networks and track their communications. In the weeks following the attack, several unencrypted discussion forums on the darknet created "threads" to identify and discuss these "infiltrators."



Thread created to discuss the "new hostile observers" on one far-right site (Darknet Forum, 2 February 2021)

In response to these alleged "hostile observers," far-right users on multiple platforms began to share strategies for how to secure their existing communication networks. One method mentioned was limiting the potential of information leakage through online posting. A post from a far-right Telegram channel recommended that users should practice good "OPSEC" and always assume that their communications will be monitored. As a result, they suggested not discussing anything online "that would incriminate themselves or others, expose sensitive information, compromise an identity." Instead, they recommended utilizing in-person communication to discuss sensitive topics.



⚠⚠**SECURITY ALERT** ⚠⚠

Please take a few minutes to "harden" or secure your Telegram account right now.

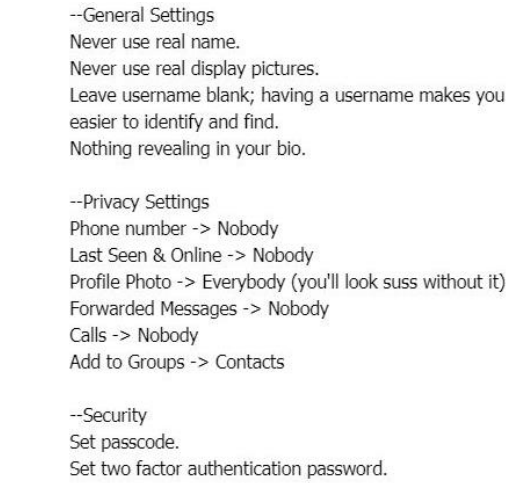
In any **public** Telegram channel your membership is *not* private. We need to operate under the assumption that both feds and members of far-left groups are monitoring all channels for information. Don't worry, though! There are a few key steps we can take to mitigate the risk of exposing personal information through Telegram:

• **ASSUME** any message you send will be read by a bad-actor. Don't say anything that would incriminate yourself or others, expose sensitive information, compromise an identity, etc.

• **DO NOT** respond to unsolicited direct messages ("DMs"). Bad-actors may try to initiate contact through direct messages in an attempt to obtain incriminating or otherwise valuable information about you and your brothers.

Telegram post discussing how to "'harden' or secure" an individual Telegram channel to limit information leakage or exposure (Telegram, 14 January 2021)

Users explored an additional level of "OPSEC" by suggesting that followers should engage in the process of "hardening" online profiles. Based on discussions from several posts, "hardening" appears to be the process of limiting the accessibility of the personally identifiable information associated with an individual user. Multiple far-right Telegram channels which promote security-related content produced guides explaining how to "harden" their profiles. Recommendations ranged from simple activities such as hiding their personal information using the privacy settings in the app to more advanced options, including registering for accounts with a phone number "that is in no way traceable."



--General Settings
Never use real name.
Never use real display pictures.
Leave username blank; having a username makes you easier to identify and find.
Nothing revealing in your bio.

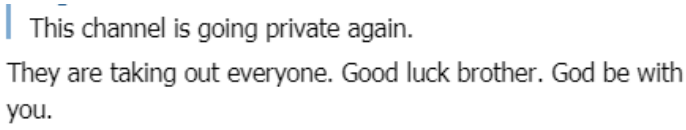
--Privacy Settings
Phone number -> Nobody
Last Seen & Online -> Nobody
Profile Photo -> Everybody (you'll look suss without it)
Forwarded Messages -> Nobody
Calls -> Nobody
Add to Groups -> Contacts

--Security
Set passcode.
Set two factor authentication password.

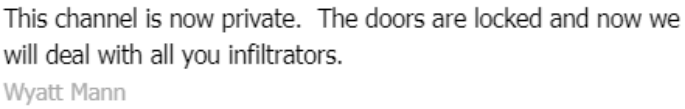
Post listing potential areas that far-right followers can utilize to "harden" their online profiles and thus limit their ability to be identified (Telegram, 3 February 2021)

Post explaining how to secure Telegram accounts to "keep your online identity, COMPLETELY secret" [sic] (Telegram, 15 May 2021)

Like "hardening" their individual online profiles, another method used by the far-right to secure their existing communications platforms against potential investigators was by "locking" the system. For example, on Telegram, many users began to privatize their channels to prevent new users from joining. Users suggested that this served two potential purposes: first, it "hides" the channel from outside users who may have been attempting to "mass report" the content; second, privatizing the channel also allows administrators to limit who can join the page, thus limiting the potential for "infiltration."



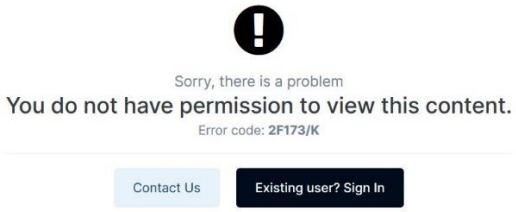
Post highlighting how users on Telegram would privatize their channel in order to avoid being "mass reported" and removed from the platform (Telegram, 23 January 2021)



Telegram post highlighting how users would privatize a channel in an effort to identify "infiltrators" who were investigating the far-right (Telegram, 13 January 2021)

While this strategy of "locking" their communication platforms originated on far-right Telegram channels, by mid-February, darknet sites associated with the far-right began to utilize the tactic as well. For example, one encrypted discussion board, whose members participated in the attack, closed; this action prevented users from discussing or accessing previously posted content. Several weeks later, the board was re-opened but required "vetting" by local administrators to ensure that any potential users were

acceptable.[18] Similarly, a militia-focused forum on the darknet, which had historically allowed anyone to view content and discussions, began to require a credentialled login to access any materials beyond the homepage.



An alert showcasing increased security measures implemented by a militia forum following the events of 6 January (Militia Message Board, 20 January 2021)

While some groups only chose to "lock" their platforms to prevent potential infiltration, other organizations utilized more drastic measures. One group, fearing the potential of being associated with the 6 January riots or infiltration, disbanded their website. The post explaining the decisions stated that the group "DID NOT CONSPIRE OR PARTICIPATE IN THE JAN 6 DC RIOTS AND CAPTIOL BREACH" [sic].

Post from a militia-focused organization website claiming that it was disbanding the website following the 6 January riots (Militia Organization Website, 21 February 2021)

ii. Migrating to More Secure Communications Platforms

In addition to securing existing communications platforms, far-right actors also began to explore the potential of migrating to more secure systems. Unlike previous posts which appeared on Telegram first and then arrived on other far-right platforms, posts calling for migration to more secure communication programs after the 6 January attack on the Capitol originated on darknet forums. Within days of the Capitol attack, members of multiple militia-focused darknet forums began advocating for utilizing different methods of communication. Several users recommended using Signal, a messaging app that offers end-to-end encryption for individuals and groups. Other posts advocated utilizing services such as "ProtonMail," an email service that similarly provides end-to-end encryption.

[18] In the lexicon of the far-right, "vetting" generally refers to the process of performing a background check on a potential recruit to and organization or group. Many organizations within the broader far-right community have discussed the importance of the "vetting" process.

[redacted] It is just not smart to gather together and even less smart to discuss the planning etc., in an insecure forum. Set this up in Signal or via protonmail. And maybe better than in person, set up a meeting on Signal, with everyone having to be vetted first before they can be added to the Signal group. And rather then bottlenecking command have a council of folks who plan and discuss strategy again via signal. And then those plans are shared via their groups. No top down command, no head to cut off, no centralization, but coordination and cooperation instead. That would achieve the same goals and a lot more of us would be interested in that than this. Or go hard head and insist it be one way or the highway. Either way, good or bad, you will achieve *something*.

Post discussing how the current tools used by the far-right to plan and communicate are "insecure," with the user recommending that far-right actors transition to "Signal" or "Protonmail" (Militia Message Board, 17 January 2021)

In addition to more secure individual communications services, far-right extremists also began to explore potential alternative platforms for group communications. Many actors rejected well-known alternatives such as Parler, Discord, or Gab, believing that those platforms "are all run by kikes and have far worse Terms of Service and censorship than even Telegram."

SECURE ALTERNATIVES TO TELEGRAM

In light of the recent increase in censorship imposed on various National Socialist and Non-Kosher channels and groups throughout Telegram, it is time we look to alternative options for communications. Parler, Discord, and Gab.ai are all run by kikes and have far worse Terms of Service and censorship than even Telegram so they're not viable options as gatekeepers and controlled opposition will try to argue. Other popular alternatives typically include Signal which is centralised and routes its servers through (((Google))) as well as Wire which routes theirs through (((Amazon))) so both have been rejected as suitable platforms.

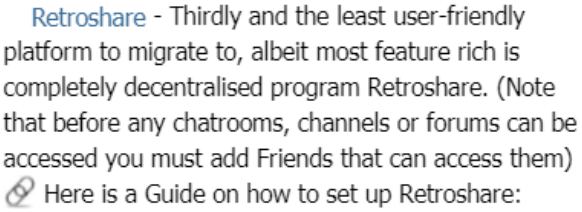
Post suggesting that the traditional communication methods utilized by the far-right, including Telegram, Parler, Gab, and Discord, are controlled by "kikes" and thus not acceptable for secure communications (Telegram, 24 January 2021)

Having rejected these more traditional venues utilized by the far-right, actors began to explore lesser-known platforms such as "Matrix." "Matrix" is an open-source messaging protocol that allows users to engage in decentralized, end-to-end encrypted communication. Using the "Element" web application, far-right actors began to utilize the "Matrix" protocol to create communal chatrooms which could only be accessed through login credentials.

Matrix - Primarily, all of us are migrating to Riot/Matrix servers using Element, which is a user friendly, decentralised and encrypted chat API for Matrix.
🔗 Join our chatroom directly here:
[redacted]

Post from a well-known far-right Telegram channel explaining that they would begin using the "Matrix" protocol to offer a "decentralized and encrypted" chatroom (Telegram, 24 January 2021)

In addition to "Matrix," users also began to explore platforms such as "Retroshare." "Retroshare," like "Matrix," is a protocol that allows users to engage in end-to-end encrypted communications but has the added benefit of limiting the potential individuals who can view the material shared. For instance, while Telegram allows nearly anyone to join a particular "channel" and thus gain access to the information posted, a "Retroshare" user has to invite other users to view their posted material; theoretically, this would "automatically limit intrusions."[19] Far-right users expressed considerable interest in the utility of this platform, even sharing guides for how to open a "Retroshare" account.


Retroshare - Thirdly and the least user-friendly platform to migrate to, albeit most feature rich is completely decentralised program Retroshare. (Note that before any chatrooms, channels or forums can be accessed you must add Friends that can access them)
Here is a Guide on how to set up Retroshare:

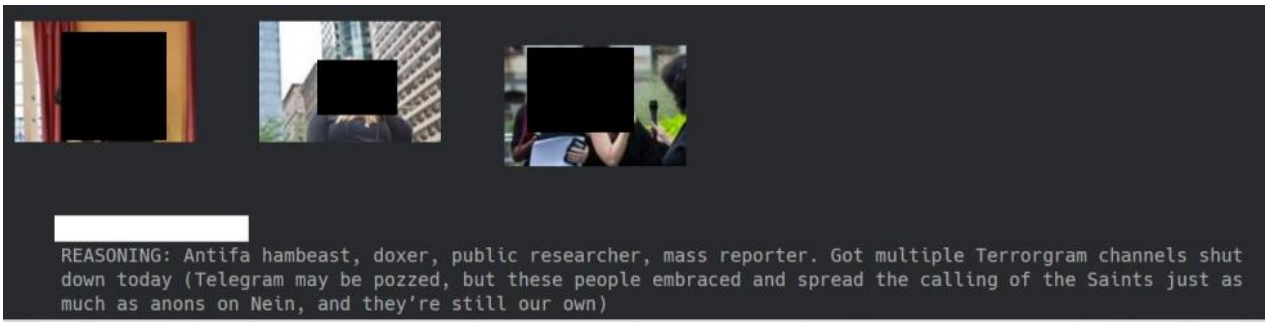
Telegram post explaining the utility of "Retroshare" as a "completely decentralized program" (Telegram, 24 January 2021)

By mid-February 2021, the far-right focus on securing existing communication platforms had again migrated, this time to white supremacists-focused darknet forums. Like their predecessors on militia-focused darknet forums and Telegram channels, the white supremacist message boards examined alternative methods for individual and group communications. In response to a more extensive discussion trend on one forum regarding the potential for "infiltrators," one user shared a detailed explanation of the security effectiveness of many platforms utilized by the far-right. The user systematically explained the strengths and weaknesses of each communication method and made recommendations for which services should be used.

iii. Countering Potential Investigators

In addition to securing existing lines of communication and exploring alternative communications platforms, far-right actors have also attempted to engage in individuals acts and coordinated campaigns to limit the ability of potential investigators to gain intelligence from their communications. Far-right actors have primarily attempted this through two methods: (i) doxing potential investigators, (ii) identifying or reporting potential investigators. Unlike many of the recent trends in far-right online strategies, which seem to first appear on Telegram and migrate to other platforms, the tactic of attempting to dox potential investigators appears to have originated on several darknet forums. There, users began to identify potential investigators and shared personal information such as images, phone numbers, addresses, and online profiles.

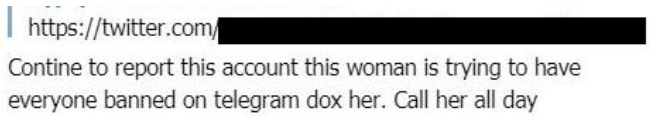
[19] Bruce Byfield, "RetroShare: Is a Private Network Useful for Privacy and Security?," Linux Magazine, accessed June 7, 2021, https://www.linux-magazine.com/Online/Features/RetroShare.



Post doxing an alleged member of "Antifa" who was investigating far-right online channels following the 6 January attack on the U.S. Capitol[20] (Darknet Forum, 12 January 2021)

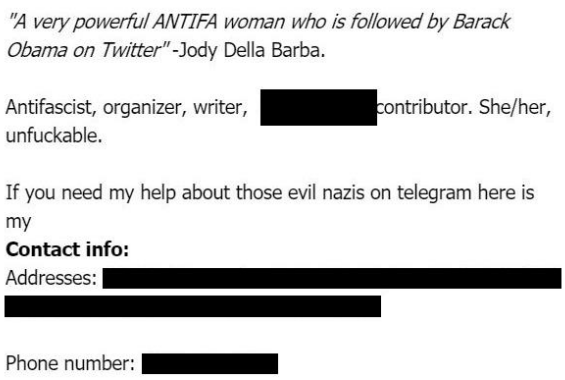
Post doxing an individual who identified and reported her "mother, aunt, and uncle" who attended the 6 January attack (Darknet Forum, 12 January 2021)

Like other strategies, doxing of investigators eventually migrated from darknet forums to well-known Telegram channels as well. There, the far-right extremists called for an escalation in doxing by suggesting that far-right actors should harass the individuals, with one post asking their followers to "call [the target] all day."



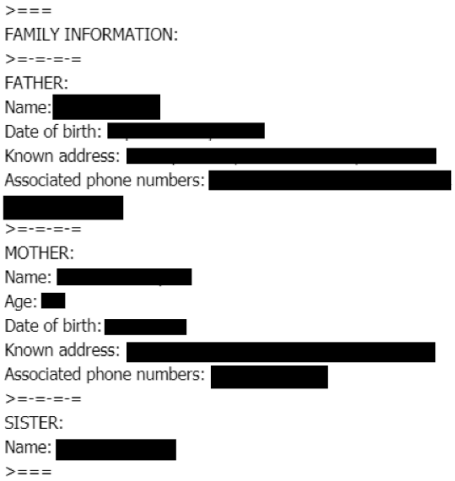
Post from a well-known far-right channel urging supporters to engage in coordinated doxing and harassment campaign against a potential investigator by "call[ing] her all day" (Telegram, 13 January 2021)

[20] Personally identifying details of the victims of doxing have been covered or omitted to protect their privacy.



Post doxing a potential investigator, wherein the user impersonated the target and then provided their work address, home address, and phone number (Telegram, 21 January 2021)

Another escalation in doxing from the far-right is in the type of information released. Whereas in the past, doxing has only been the intentional identification or publication "of private information" about the intended target, far-right channels on Telegram escalated the strategy by releasing personally identifiable information on their intended targets and their families as well.[21] For example, one post that was repeatedly shared by far-right channels released the personal information of an intended target, their parents and siblings.

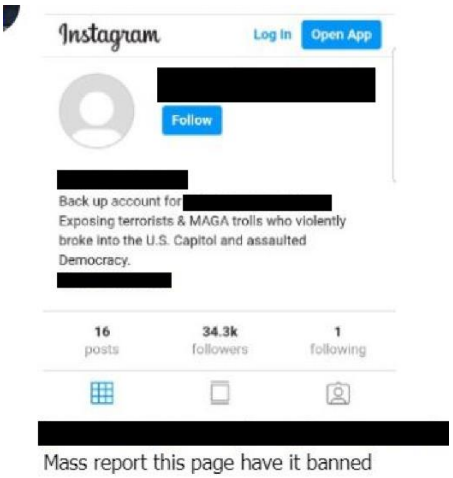


Post showing an escalation of the far-right by doxing the family of an intended target (Telegram, 24 January 2021)

In addition to doxing, far-right extremists also regularly attempted to identify individuals who were investigating potential far-right links to the 6 January riot. Once they had been identified, users attempted to organize coordinated "mass reporting" campaigns in order to have the accounts of potential investigators frozen or removed. For instance, two days after the Capitol attack, a well-known far-right channel asked its supporters to "mass report" an Instagram account that was attempting to identify any of the individuals who

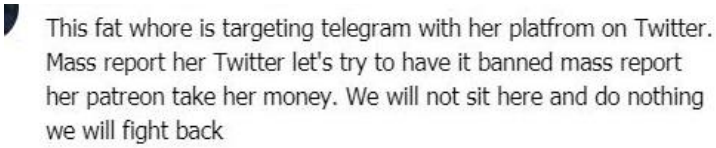
[21] Doxing is generally defined as "to publicly identify or publish private information about (someone) especially as a form of punishment or revenge" For further explanation, see: "Dox," Merriam-Webster (Merriam-Webster), accessed June 7, 2021, https://www.merriam-webster.com/dictionary/dox.

were involved in the unrest. Similarly, several channels called on supporters to "mass report" an individual who was actively reporting on "White Nationalist pages on Telegram."



Post urging followers to engage in a coordinated campaign to "mass report" an Instagram page to "have it banned" (Telegram, 8 January 2021)

Post advocating for a coordinated campaign to "mass report" an individual who was "reporting White Nationalist pages on Telegram" (Telegram, 12 January 2021)



Post encouraging an organized campaign to "mass report [a potential investigator's] Twitter" in order "to have it banned" (Telegram, 13 January 2021)

Conclusion and Policy Implications

In the nearly six months since the 6 January attack, several events have occurred. First, more than 70,000 accounts across the major social media platforms were suspended or removed.[22] Second, a

[22] "Social Media Crackdown Continues After Siege of US Capitol," U.S. News & World Report (U.S. News & World Report, January 12, 2021), https://www.usnews.com/news/politics/articles/2021-01-12/social-media-crackdown-continues-after-siege-of-us-capitol.

Congressional Commission was considered to investigate and better understand the underlying causes of the Capitol attack.[23] Third, the Department of Justice launched the "largest criminal investigation" in its history, which ultimately resulted in the arrest of more than 465 individuals that were involved in the attack.[24] Given these subsequent events, far-right actors have become increasingly concerned with their safety in cyberspace and adjusted their online activity accordingly.

Immediately following the attack, far-right actors adopted a more defensive posture in their online communications. Specifically, far-right extremists engaged in two defensive actions: (i) securing existing lines of communication, (ii) locating and migrating to more secure communication platforms. In addition to their defensive posture, far-right extremists also began implementing an offensive strategy to locate and counter potential investigators using two types of action: (i) identifying and doxing, (ii) organizing "mass reporting" campaigns to de-platform potential investigators. While such activities were initially only a response to the Capitol attack, the behaviors have persisted throughout the subsequent months. Given these strategies' continued use, it is believed that the Capitol attack and subsequent scrutiny have substantially altered the broader far-right's behavior in cyberspace. This change has significant policy implications.

As far-right individuals and groups continue to migrate towards and utilize more secure platforms, it will be increasingly challenging to monitor their communications. Given this added difficulty, intelligence collection and analysis opportunities may decrease. As multiple reports suggest that the Capitol attack was planned openly online, it is troubling to consider the potential actions of far-right extremists should their communications be allowed to continue without monitoring.[25]

Given its durability over time, the movement of the American far-right towards more security and discretion in cyberspace seems to be a permanent or semi-permanent change in their online strategic behavior. As the Biden Administration allocates "$100m in additional resources for analysts, investigators, prosecutors, and other personnel and resources to thwart domestic terrorism," these individuals must be aware of this strategic change and determine new methods to monitor far-right actors online.[26] Failure to do so may allow extremist actors to plan, organize, and execute future attacks.

---

[23] Brian Naylor, "Senate Republicans Block A Plan For An Independent Commission On Jan. 6 Capitol Riot," NPR (NPR, May 28, 2021), https://www.npr.org/2021/05/28/1000524897/senate-republicans-block-plan-for-independent-commission-on-jan-6-capitol-riot.

[24] Alexander Mallin, "150 Days after Capitol Attack, More than 465 Arrested as FBI Seeks Tips on Hundreds More: DOJ," ABC News (ABC News Network, June 5, 2021), https://abcnews.go.com/Politics/150-days-capitol-attack-465-arrested-fbi-seeks/story?id=78103940&utm_source=iterable&utm_medium=email&utm_campaign=2430856_.

[25] Laurel Wamsley, "On Far-Right Websites, Plans To Storm Capitol Were Made In Plain Sight," NPR (NPR, January 8, 2021), https://www.npr.org/sections/insurrection-at-the-capitol/2021/01/07/954671745/on-far-right-websites-plans-to-storm-capitol-were-made-in-plain-sight.

[26] Smith, "White House Unveils First National Strategy to Fight Domestic Terrorism," June 15, 2021.

ABOUT THE ICT

Founded in 1996, the International Institute for Counter-Terrorism (ICT) is one of the leading academic institutes for counter-terrorism in the world, facilitating international cooperation in the global struggle against terrorism. ICT is an independent think tank providing expertise in terrorism, counter-terrorism, homeland security, threat vulnerability and risk assessment, intelligence analysis and national security and defense policy.

ICT is a non-profit organization located at the Interdisciplinary Center (IDC), Herzliya, Israel which relies exclusively on private donations and revenue from events, projects and programs.