FLASHPOINT

Why Niche Social Data Matters for Counter-Terror Initiatives

Introduction

For years, the dark web has been touted as a valuable intelligence source for governments focused on counter-terror initiatives. According to a report published by the Henry Jackson Society in 2018, the dark web is a reliable source for locating and understanding terrorist recruitment, propaganda, and cryptocurrency exchange.

Dark websites like The Daily Stormer, 8kun,[1] and marketplaces selling fake passports, are obvious enablers for violent extremists and terrorists. More recently, the dark web has been identified by some as an overlooked platform as governments and technology companies collaborate to take down extremist content on the internet—particularly on mainstream platforms like YouTube, Facebook, and Twitter.

Additionally, some less obvious social media networks are becoming more actively used by extremist communities and are as crucial as the dark web in supporting counter-extremist missions. These networks are particularly useful for tracking and understanding extremists in less-understood but highly dangerous groups, such as incels and other evolving extremist branches.

This case study explores how these social networks can be accessed and what their value is to organizations working in this space by looking at incel extremism online.

Relevant Social Networks for Counter-Extremism

Methods of radicalization are evolving quickly. This is true across a number of dangerous groups, from ISIS to alt-right communities, and single-issue extremism like the “manosphere.” More of these communities are migrating to niche, less-regulated networks as widely used social media sites like Facebook crack down on extremist content. While some of these (e.g. 8kun, Endchan) are hosted on the dark web, alternative platforms like Telegram, 4chan, Gab, and Mastodon are gaining popularity.

While Telegram has censored Islamist terrorism on its network, other extremist groups are still highly active on the popular chat application. Sites like Gab and Mastodon are built using a decentralized model, which makes them virtually impossible to remove or moderate regardless of the type of content they host.

These social media sites are more user-friendly than dark web navigation even though they don’t achieve the same level of anonymity as a Tor browser. In general, these sites are more effective for reaching younger audiences who are vulnerable to radicalization.

[1] 8kun is the successor of 8chan, which was moved to the dark web shortly after publishing a manifesto linked to the 2019 mass shooting in El Paso, Texas.

For government, defense, and other organizations working in counter-terrorism and extremism, these social media networks are useful for locating:

- **Extremist manifestos, leakage patterns, and other warning signs**
- **Recruitment initiatives and tactics**
- **Extremist propaganda**
- **Language and colloquialisms unique to specific terrorist and extremist groups**
- **Emerging and less-understood extremist ideologies and motives**

This information is highly valuable for predicting real public safety threats. It's also useful for identifying vulnerable individuals, understanding how and why extremists operate, and improving overall awareness of these communities to better inform counter-terror initiatives.

Barriers to Accessing Extremism on Social Media

Defense ministries and other entities working in counter-terror rely on data aggregation platforms and APIs to collect and process publicly-available information across the web. Many commercial, off-the-shelf tools and APIs offer these users access to dark web and social media data from more mainstream sites like YouTube and Twitter.

However, many existing solutions do not offer niche social media coverage for alternative networks like those mentioned. Additionally, commercial solutions often prioritize streaming real-time data rather than providing well-maintained data lakes and historical repositories. These are necessary for advanced defense applications associated with counter-extremism, such as data integrations and machine learning.

These capabilities are valuable for detecting the colloquialisms and intentional obfuscation typical of online extremism. Analysts need these capabilities to more efficiently understand patterns in online extremism, especially as extremist groups become more overlapped, fluid, and complex in their online interactions.

Case Study: Understanding Incel Extremism

Background

To explore the value of accessing alternative social data, an analyst was tasked with assessing incel extremism online. The term incel concatenates “involuntary” and “celibate,” and describes a group of male extremists who claim to be incapable of accessing female intimacy. Incel content is themed around violence and misogyny.

While a number of terror attacks have been committed by incels, the movement is underresearched and less understood. It is still not widely classified as an active terror group that attracts and radicalizes young men in ways similar to well-known groups like ISIS. In fact, the Terrorism and Violent Extremism Awareness Guide in Canada was revised as recently as June 2020 to include incels. The incel community also has a complex vocabulary and overlaps with other extremist groups, such as the alt-right. This makes threat detection and community awareness challenging for intelligence analysts.

Information gathered from niche social media platforms can be leveraged in counter-terror missions to anticipate public safety threats, engage with users susceptible to radicalization, and better understand incel communities as organized movements.

Process

The analyst used the Flashpoint API to gather data across a number of niche social platforms, including Telegram, Gab, 4chan, and others. They chose to navigate this information within Echosec, Flashpoint’s open-source intelligence solution. However, if the analyst was working outside of Echosec—for example, through proprietary software—they could also submit API queries and access social data through their own software.

The analyst focused on known incel keyphrases, particularly those considered high-risk. For example, tense variations of the phrase “go ER” (“go Elliot Rodger”), which implies suicidality and an intent to act out violently in public. The analyst also queried the keyphrase “praise the saints,” which is used by extremists to reference and revere past shooters.

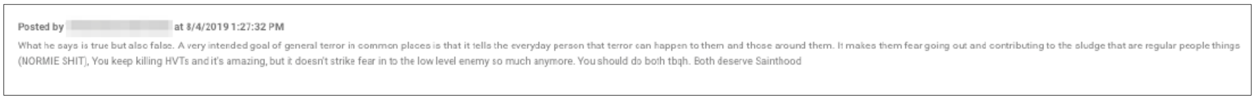
These are both examples of leakage—a subtle (or not-so-subtle) hint preceding an attack. In a 2019 report analyzing shooter activity and behavioral patterns in the US, social media use, leakage, and an interest in past shooters are some of the most common warning signs and social contagion factors preceding an active shooter event.

Results

The analyst returned over 7,500 posts from Gab and Telegram repeating variations of “go ER” and “praise the saints.” As the analyst began reviewing results, they narrowed in on a specific Telegram user (named “User A” for the purpose of this case study). User A’s content was of particular interest to the analyst, as they posted in both fluent English and Russian, and used other incel terms such as “normie” and “soybean bully” in their posts.

The analyst then pivoted off of User A’s handle to narrow in on their post history within Telegram. The analyst viewed this content in Echosec without needing to set up a Telegram account, which would have otherwise been required to directly access the thread. The user’s catalog of activity included:

- **Sharing an audiobook of Anders Breivik’s manifesto**
- **Identifying ideal target goals in an act of terror**
- **Posting public USASOC documentation with the goal of informing the community about how to “evaluate, infiltrate, and organize movements”**

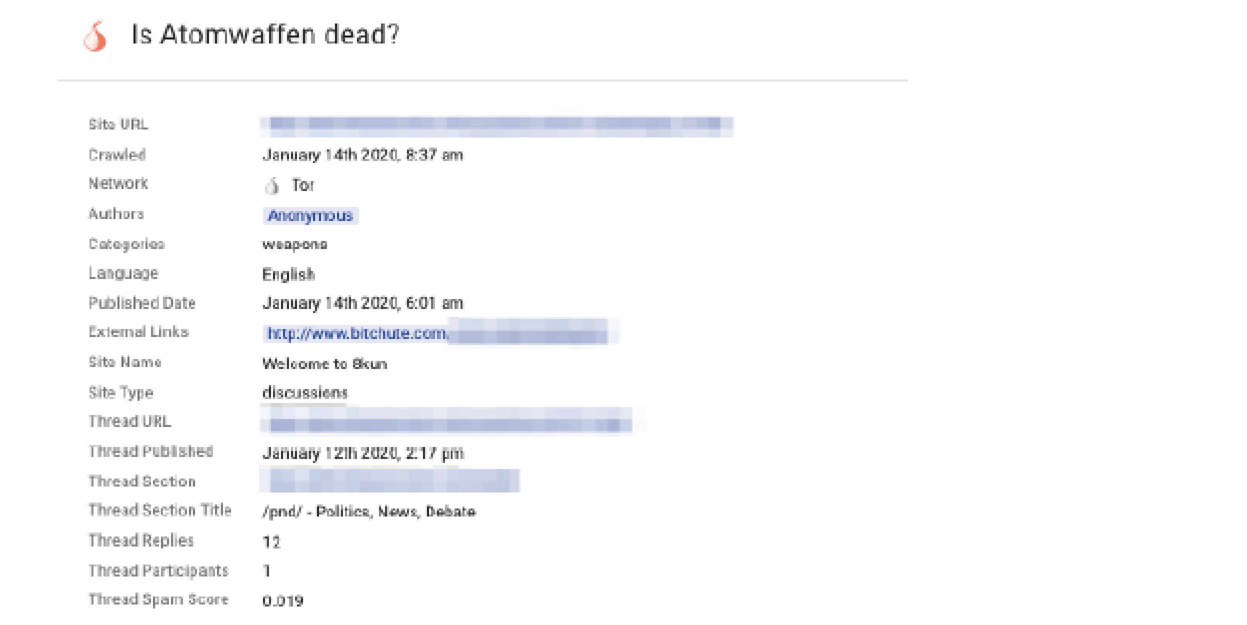


Posted by [redacted] at 8/4/2019 1:27:32 PM

What he says is true but also false. A very intended goal of general terror in common places is that it tells the everyday person that terror can happen to them and those around them. It makes them fear going out and contributing to the sludge that are regular people things (NORMIE SHIT), You keep killing HVTs and it's amazing, but it doesn't strike fear in to the low level enemy so much anymore. You should do both tbqh. Both deserve Sainthood

Telegram post by User A as viewed in Echosec: “A very intended goal of general terror in common places is that it tells the everyday person that terror can happen to them and those around them. It makes them fear going out and contributing to the sludge that are regular people things (NORMIE SHIT). You keep killing HVTs but it doesn’t strike fear in to the low level enemy so much anymore. You should do both tbqh. Both deserve Sainthood”

Based on User A’s Telegram post volume (296 posts) and the high-risk nature of their content, they appear to be fully embedded in the incel community and operating as an influencer. The analyst also cross-referenced User A’s handle across dark web sources, and found a number of posts promoting their Telegram account on 8kun:



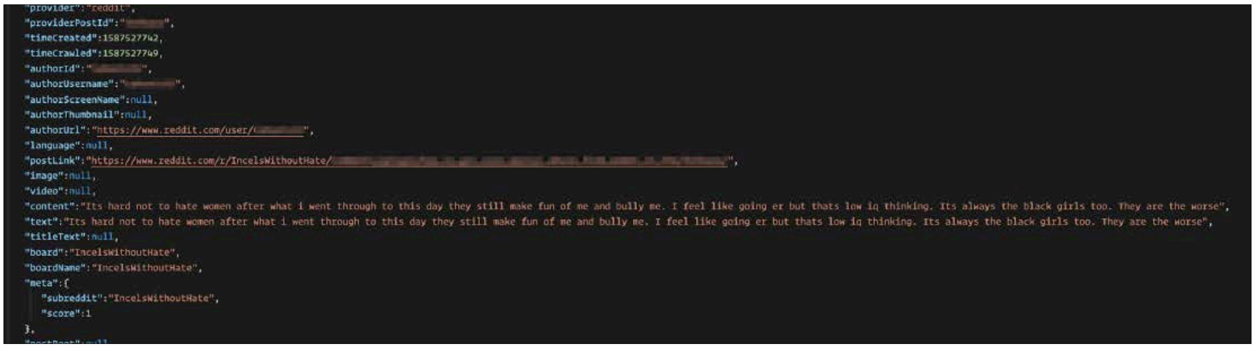
Is Atomwaffen dead?

Site URL	[redacted]
Crawled	January 14th 2020, 8:37 am
Network	Tor
Authors	Anonymous
Categories	weapons
Language	English
Published Date	January 14th 2020, 6:01 am
External Links	http://www.bitchute.com/[redacted]
Site Name	Welcome to 8kun
Site Type	discussions
Thread URL	[redacted]
Thread Published	January 12th 2020, 2:17 pm
Thread Section	[redacted]
Thread Section Title	/pnd/ - Politics, News, Debate
Thread Replies	12
Thread Participants	1
Thread Spam Score	0.019

User A promoting their Telegram account and Atomwaffen propaganda on 8kun—as viewed in Echosec

The post shown above also shares a BitChute link to an Atomwaffen propaganda video, suggesting crossover between incel and neo-Nazi ideologies.

The analyst ran a second search query, this time locating variations of “go ER” across a broader spectrum of niche social sites—including Mastodon, Raddle, and Reddit in addition to Telegram and Gab. This search returned a much narrower pool of results (101), including Reddit activity from “User B,” who expresses a desire to “go ER:”

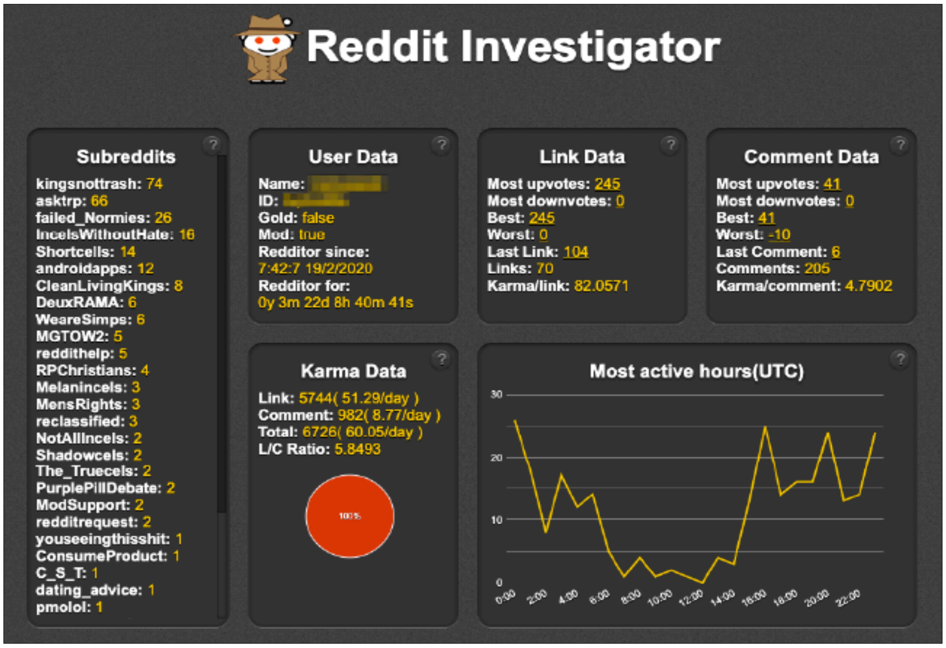


```
"provider":"reddit",
"providerPostId":"[redacted]",
"timeCreated":1587527742,
"timeCrawled":1587527749,
"authorId":"[redacted]",
"authorUsername":"[redacted]",
"authorScreenName":null,
"authorThumbnail":null,
"authorUrl":"https://www.reddit.com/user/[redacted]",
"language":null,
"postLink":"https://www.reddit.com/r/IncelsWithoutHate/[redacted]",
"image":null,
"video":null,
"content":"Its hard not to hate women after what i went through to this day they still make fun of me and bully me. I feel like going er but thats low iq thinking. Its always the black girls too. They are the worse",
"text":"Its hard not to hate women after what i went through to this day they still make fun of me and bully me. I feel like going er but thats low iq thinking. Its always the black girls too. They are the worse",
"titleText":null,
"board":"IncelsWithoutHate",
"boardName":"IncelsWithoutHate",
"meta":{
    "subreddit":"IncelsWithoutHate",
    "score":1
},
```

User B post shown as a JSON API query result: “Its hard not to hate women after what i went through to this day they still make fun of me and bully me. I feel like going er…”

Pivoting off of User B allowed the analyst to view their other online activity, which was only on Reddit. They were able to determine that the user is likely high-school-aged based on their other posts (“Girls in my high school…”). An external OSINT tool, Reddit Investigator, enabled the analyst to identify a number of incel subreddits where User B is engaged as well as other activity patterns:

User B appears to be a minor, new to the incel community, and relatively active on Reddit. They fall into a category of individuals vulnerable to radicalization by more embedded influencers such as User A. If radicalized, they are also likely to move to less-regulated networks and potentially adopt other extremist ideologies.



Reddit Investigator

Subreddits

kingsnottrash:	74
asktrp:	66
failed_Normies:	26
IncelsWithoutHate:	16
Shortcells:	14
androidapps:	12
CleanLivingKings:	8
DeuxRAMA:	6
WeareSimps:	6
MGTOW2:	5
reddithelp:	5
RPChristians:	4
Melanincels:	3
MensRights:	3
reclassified:	3
NotAllIncels:	2
Shadowcels:	2
The_Truecels:	2
PurplePillDebate:	2
ModSupport:	2
redditrequest:	2
youseeingthisshit:	1
ConsumeProduct:	1
C_S_T:	1
dating_advice:	1
pmolol:	1

User Data

Name: [redacted]
ID: [redacted]
Gold: false
Mod: true
Redditor since:
7:42:7 19/2/2020
Redditor for:
0y 3m 22d 8h 40m 41s

Link Data

Most upvotes: 245
Most downvotes: 0
Best: 245
Worst: 0
Last Link: 104
Links: 70
Karma/link: 82.0571

Comment Data

Most upvotes: 41
Most downvotes: 0
Best: 41
Worst: -10
Last Comment: 6
Comments: 205
Karma/comment: 4.7902

Karma Data

Link: 5744(51.29/day)
Comment: 982(8.77/day)
Total: 6726(60.05/day)
L/C Ratio: 5.8493

Most active hours(UTC)

Defense intelligence analysts can use this information to easily identify extremist networks, high-risk individuals like User A, as well as threat indicators (“I feel like going er”) on more niche sites. While the dark web is useful for investigating terrorism and extremism, obscure social media platforms are where users are more likely to enter and engage in these communities.

This information was acquired without needing to directly access any social networks or set up fake accounts, even on Telegram threads that require membership to access. The analyst was able to easily search and navigate this information within Echosec, avoiding any security issues. If necessary, the social data could also be accessed through an external interface or used for more advanced applications via the Flashpoint API. For example, this would allow data scientists in defense to build machine learning models that detect colloquial language, leakage, and other threat indicators specific to extremist groups.

Conclusion

Extremism is rapidly evolving online—both as communication and recruitment tactics advance and as branches of extremism develop and overlap. This presents many challenges for analysts and data scientists working in government and defense. For one, these communities have complex, novel communication methods that are difficult and time-consuming to analyze.

Secondly, their activity occurs not just on the dark web, but on niche social media platforms that are not commonly available through commercial search tools. APIs that specialize in accessing niche data from these sources are crucial for driving counter-terror and national security missions alongside other data feeds. This technology will not only glean more insights about extremist networks, but also enable data scientists to build advanced applications increasingly required by defense teams, such as machine learning.

Governments and technology giants worldwide are ramping up their efforts to address online extremism through initiatives like The Christchurch Call. But not all social media platforms can easily be regulated or dismantled. As shown through the incel example above, accessing these sources is crucial for expanding counter-terror solutions beyond censorship.

> "Increasing awareness of extremism, enhancing communication with vulnerable communities, pursuing scientifically sound research, expanding socio-economic development, implementing innovative de-radicalization or de-engagement initiatives, and re-evaluating definitions of extremism are all, to some extent, part of the package."
>
> *— Daniil Davydoff, Associate Director of Intelligence at AT-RISK International (from The Rise of Extremism, Security Magazine)*

ABOUT FLASHPOINT

Trusted by governments, commercial enterprises, and educational institutions worldwide, Flashpoint helps organizations protect their most critical assets, infrastructure, and stakeholders from security risks such as cyber threats, ransomware, fraud, physical threats, and more. Leading security practitioners—including physical and corporate security, cyber threat intelligence (CTI), vulnerability management, and vendor risk management teams—rely on the Flashpoint Intelligence Platform, comprising open source (OSINT) and closed intelligence, to proactively identify and mitigate risk and stay ahead of the evolving threat landscape. Learn more at www.flashpoint.io.

Learn more about
our solutions

Book a Call