Hiding in Plain Sight: White Extremists and Rogue Wolves In the Margins of the Internet

Kathleen Moore[1], Lisa Colelli[2], Ariel Kennedy[3], Emma Leonard[4]

[1] Intelligence Analysis Program, James Madison University, Harrisonburg, VA 22807
moore8ka@jmu.edu
[2] Intelligence Analysis Program, James Madison University, Harrisonburg, VA 22807
colelllc@dukes.jmu.edu
[3] Intelligence Analysis Program, James Madison University, Harrisonburg, VA 22807
kenne5am@dukes.jmu.edu
[4] Intelligence Analysis Program, James Madison University, Harrisonburg, VA 22807
leonarek@dukes.jmu.edu

Abstract. Since the violence of the Unite of the Right rally in Charlottesville, Virginia in August 2017, tech companies have bowed to pressure removing white extremist groups from their platforms. This prompted concerns that extremist organizations would re-locate to Dark Web where their activities could occur unencumbered by law enforcement or social pressure common on Surface Web. This work examines the Internet presence of 150 white extremist groups in the United States, finding little presence on Dark Web, with most groups preferring member-only Surface sites, using innovative language and visual techniques to evade detection in Surface Web social media services. While lack of group presence appears encouraging, their influence on individual actors causes concern.

Keywords: White Extremism, Surface Web, Dark Web

1 Introduction

Since 2016, the concern of rising populist factions and the re-emergence of white nationalist, white supremacy, and Neo-Nazi groups (heretofore referenced as "white extremists") in the United States (US) were largely ignored by local, state and federal law enforcement. Instead, efforts remained focused on foreign-based terrorism, a hold-over from the September 11 attacks fifteen years before [1]. A change in perspective and focus by the police did not occur until after the Unite the Right Rally in Charlottesville, Virginia on 11 August, 2017 that resulted in the death of one protester, two policemen, and fifteen injured persons [2]. The rally seemed to crystalize a realization that race-based hate crimes, both perpetrated and foiled, had been on a steady increase in the US for the last decade [3].

Until this time, white extremist groups used Surface Web sites to recruit, communicate, and in the case of the Unite the Right rally, coordinate violent activities [4]. Public furor and commercial pressure resulted in private, US-based tech companies

no longer permitting these groups to use their services [5]. Google, Facebook, Twitter, GoDaddy, Reddit, and Discord all refused access to groups espousing racist ideology. The removal of these groups prompted concerns that this move would force a migration of their communications from the Surface Web to Dark Web, and would hinder law enforcement's ability to track and monitor potentially violent groups and their coordinating activities.

The concerns regarding Dark Web migration is well-founded. The Dark Web is an area of the Internet requiring special technology, different search strategies, and lacks the overall inter-connectedness of the Surface Web making navigation of this space and information discovery difficult. Further, this space anonymizes IP addresses making identification of person on the Dark Web difficult. While the United States Navy invented the technology of the Dark Web for activists, journalists, dissidents, and persons concerned with government monitoring, it has also become a haven for illegal market activity and terrorists, with most law enforcement professionals lacking the knowledge or skill to monitor this space [6]. Given these concerns, this works seeks to establish the actual footprint of the groups of concern across the spectrum of the Internet, and to determine these groups' level of activity on the Dark Web.

2 Data and Methods

This study examines the overall Internet presence of 150 US-based, active groups along with recognized public figures on behalf of their movement. These organizations were chosen based on their designation as "hate groups" by the Southern Poverty Law Center, an American nonprofit legal advocacy organization specializing in civil rights and public interest litigation that also monitors extremist groups across the country [7]. White rooted in racism, ideology among these organizations differ. Fifty-five of these groups identify as white nationalist or supremacists, 28 as Neo-Nazi, 27 as Ku Klux Klan and racist skinhead respectively, 7 as Holocaust Deniers, and 6 as Neo-Confederates.

Table 1. Matrix of groups and spokespersons Internet presence.

Group-Name	Identity	.net	.org	.com	Youtube	Youtube-Channel	Facebook	Twitter	Instagram	Discord	Gab	Reddit	4chan	8chan	.onion	Forums-Found-in-DB	Message-Boards	Other-Chans	DB Number-Hits
Crew 38	Racist Skinhead	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Deir Yassin Remembered	Holocaust Denial	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
Die Auserwahlten	Racist Skinhead	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Dixie Republic	Neo-Confederate	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
East Coast Knights of the True Invisible Empire	Ku Klux Klan	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	5
Eastern Hammerskins	Racist Skinhead	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
Endangered Souls RC/Crew 519	Neo-Nazi	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Exalted Knights of the Ku Klux Klan	Ku Klux Klan	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Faith and Heritage	White Nationalist	0	0	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	1
Firm 22	Racist Skinhead	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Forza Nuova	White Nationalist	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	162
Foundation for the Marketplace of Ideas	White Nationalist	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Free American	White Nationalist	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	15
Ghost	Neo-Nazi	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	355
Global Crusaders: Order of the Ku Klux Klan	Ku Klux Klan	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Golden Dawn	Neo-Nazi	0	0	1	1		0	0	0	0	0	1	0	0	0	0	0	0	824
Golden State Skinheads	Racist Skinhead	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
Golden-State 45/Kindred 45	Racist Skinhead	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
GoyFundMe	White Nationalist	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	5
H.L. Mencken Club	White Nationalist	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
Identity Dixie	Neo-Confederate	0	0	1	0	0	0	1	1	0	1	0	0	0	0	0	0	0	1
Identity Evropa	White Nationalist	0	0	1	1	1	0	0	1	0	1	1	0	0	0	0	0	0	25
Institute for Historical Review	Holocaust Denial	0	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	12
International Keystone Knights of the Ku Klux Klan	Ku Klux Klan	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Irving Books	Holocaust Denial	0	0	1	0	0	1	1	0	0	0	0	0	0	0	1	0	0	6
Keystone United	Racist Skinhead	0	0	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	5
Knights of the Ku Klux Klan	Ku Klux Klan	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	28
Knights of the White Disciples	Ku Klux Klan	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7
League of the South	Neo-Confederate	0	1	1	1	0		0	0	0	0	1	1	0	0	0	0	0	47
Loyal White Knights of the Ku Klux Klan	Ku Klux Klan	0	0		0	1	0	0	0	0	0	1	0	0	0	0	0	0	25

Key-word searches based on group name and recognized leaders, such as Richard Spencer and others, was performed on both Surface and Dark Web. Surface Web presence was examined for general web sites (.com, .net, .org), social media presence (Facebook, Twitter, Instagram), video channel (YouTube), members-only access sites (Discord, Gab), and chans (4chan, 8chan). Dark Web presence was examined for onion sites (.onion), forums, message boards, chans, and members-only access sites. A matrix was created to organize findings, and later, used as a database for social network analysis (see Table 1).

Social Network analysis was then performed using NodeXL to visualize their connectivity across the Internet. Figure 2 shows areas of Internet presence from a broad perspective of groupings: Dark Web (DW), Surface Web Sites (SWS), Surface Web Social Media (SWSM), and Surface Web Members only (SWMO).

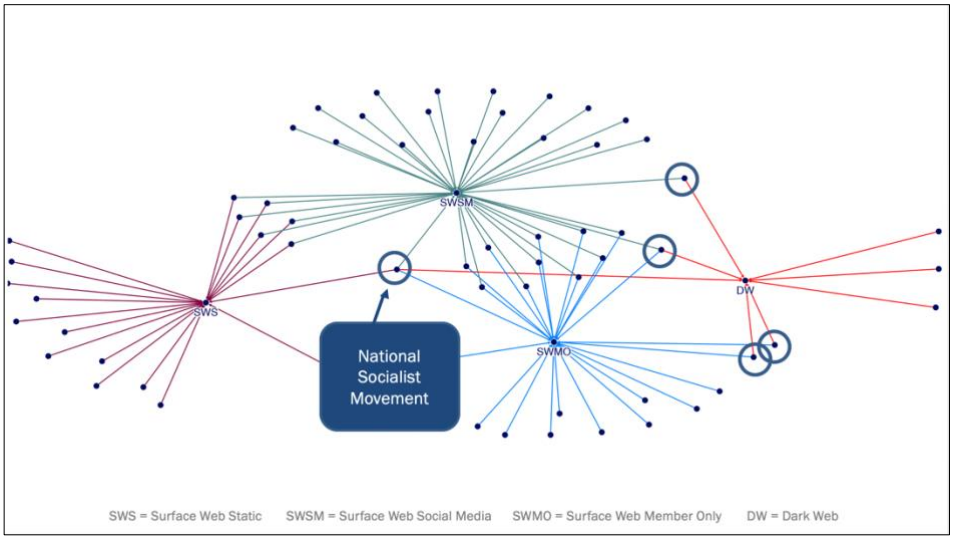

Fig. 1. Network analysis revealed little presence of white extremist groups on Dark Web.

3 Analysis

The keyword search yielded 32,150 mentions of various white extremist groups on Dark Web, however, revealed the presence of very few actual Dark Web (DW) sites (see Figure 1) as only eight groups were identified as having a site in this space. In fact, when the various types of presence are grouped broadly, there is very little overlap across the spectrum. Most groups have either a Surface Web Static Site (SWST) and Surface Web Social Media (SWSM), or a site and Surface Web Members Only (SWMO) presence. Across the spectrum, 26% of these groups had a Facebook page (levels of activity differed), 23% had one or more Surface Web sites, and 4% actively use 8chan or have an active thread.

Only one organization, the National Socialist Movement, had a presence across all four categories, however, did not have any recent activity with some sites and accounts effectively lying dormant.

On both Surface Web and Dark Web, there was witnessed a tendency towards those who post white extremist ideology and messaging to not identify as affiliated with any particular organization. There is expressed agreement, support, or admiration without explicit statements of membership. On Dark Web, these individuals mostly occupy forums and chans, while on Surface Web, they are active most active in Twitter. The individuals using public social media such as Twitter, employ a special type of coded language (see Figure 2). This particular style of language uses common, everyday words that are imbued with alternate meanings. For example, among white extremists on Twitter, they will use the words *skittle*, *google*, and *skype* as replacements for Muslims, persons of color, or Jewish persons. These words evade Twitter's filters, appear confusing to others not in the know, and create noise in which to hide their signal.

Fig. 2. White extremists on Twitter using common words imbued with racist meanings.

This style of language differs from the known lexicon of most groups, which means they have not violated most tech companies' service agreements, and thus, this allows them to remain on Surface Web sites unencumbered by either company censors or burdened by opposing social pressure. Additionally, we see some groups, such as the Patriot Front, using imagery to express themselves that also evades keyword filters from tech companies and large-scale public scrutiny (see Figure 3).

Fig. 3. The Patriot Front uses explicit imagery on Twitter which evades tech company filters.

Other wishing to express themselves more freely on Surface Web without protest have instead migrated to members-only forum sites such as Gab, or created static, members-only Surface Web sites. Though these sites are still subject to infiltration, white extremist groups remain on these platforms largely unhindered by public protest.

4 Discussion

The results of this research yielded similar results to research performed on foreign-based terrorist organizations where it was shown that foreign-based terrorist groups exhibiting the same type of dispersal across the Internet spectrum [8]. Overall, none of the groups identified for this study appears to be fully optimizing the tools available to them via the Internet as a whole. Possible explanations for this may be that Dark Web is too cumbersome technologically for many extremist group members, and the ease of use of Surface Web requires minimal modification of language or behavior to remain active and continue spreading ideology.

Further, the greater exposure of Surface Webs allows such groups the ability to engage in trolling behavior in order to agitate and more easily recruit future members, thus using coded language and imagery to "shitpost" is easily done as these social media platforms are well-embedded in the culture [9].

Though the large-scale absence on Dark Web by white extremist groups may be viewed as good news for law enforcement officials that are largely unskilled and overwhelmed by the Dark Web, there still remains a threat in the coded language used by these groups and whether that may be related to coordination of violent activity. Further, while formal group-level organization appears to be low at present, there is growing anecdotal evidence of these sites inspiring individual actors, such as the instances of the 2018 synagogue massacre in Pittsburgh, Pennsylvania, USA, the two mosque attacks in Christchurch, New Zealand [10][11], and the synagogue shooting in San Diego in 2019 [12]. Commonly referred to as "lone wolves" we identify them instead as "rogue wolves" as their online activities prior to violent acts often shows a

rich history of interaction by participation in online, white extremist sites, forums, and social media [13]. Though loosely connected, and not identified as affiliated to any particular organizations, these "rogue wolves" clearly draw inspiration from these communities as evidenced by published manifestos of these individual actors prior to their violent actions.

5 Future Work

Based on the findings of this work, future research will be performed at both the Surface and Dark Web level. As the Surface level, analysis will be performed on possible patterns between use of coded words and the emojis often used in conjunction (see Figure 2). If discernible patterns exist, this may provide a way for researchers to separate meaningful posts from random utterances on social media.

Additionally, a thorough analysis of individual postings across the various message boards, forums, and chans on Dark Web may provide better insight into information flow in that space.

Lastly, further research is required to understand the relationship between online hate group messaging and propaganda and single-actor (rogue wolf) activity.

6 Limitations

Since the Dark Web lacks the inter-connectedness of Surface Web, and also lacks search engines, there may be a possibility that white extremist sites may be present but not yet detected. Further, as stated, the difference between explicit and implicit language also opens the possibility that not all sites were detected on Surface Web.

References

1. Reitman, J. U.S. Law Enforcement Failed to See the Threat of White Nationalism. Now They Don't Know How to Stop It. New York Times. https://www.nytimes.com/2018/11/03/magazine/FBI-charlottesville-white-nationalism-far-right.html, last accessed 2019/05/08.
2. Heim, J. Recounting a day of rage, hate, violence, and death. Washington Post, https://www.washingtonpost.com/graphics/2017/local/charlottesville-timeline/?utm_term=.292cd1d20dd8, last accessed 2019/05/08.
3. Beirich, H. White Supremacy flourishes amid fears of immigration and nation's shifting demographics. Southern Poverty Law Center Intelligence Report, https://www.splcenter.org/fighting-hate/intelligence-report/2019/year-hate-rage-against-change, last accessed 2019/05/08.
4. Roose, K. This Was the Alt-Right's Favorite Chat App. Then Came Charlottesville. The New York Times, https://www.nytimes.com/2017/08/15/technology/discord-chat-app-alt-right.html, last accessed 2019/05/08.
5. Morris, C. All the Companies Who Say Hat Groups Can't Use Their Services Anymore. Fortune, http://fortune.com/2017/08/17/hate-groups-google-godaddy-apple-paypal/, last accessed 2019/05/08.

6. Davis, C. Addressing the Challenges of Enforcing the Law on the Dark Web, Global Justice Blog, https://www.law.utah.edu/addressing-the-challenges-of-enforcing-the-law-on-the-dark-web/, last accessed 2019/05/08.
7. Southern Poverty Law Center Hate Map, https://www.splcenter.org/hate-map, last accessed 2019/05/08.
8. Tirados, A. Dark Networks: Social Networks Analysis of Dark Web Communities. Recorded Future, https://www.recordedfuture.com/dark-web-networks/, last accessed 2019/05/08.
9. Bogost, I. The Meme Terrorists. The Atlantic, https://www.theatlantic.com/technology/archive/2019/04/california-synagogue-shooting-worse-you-thought/588352/, last accessed 2019/05/08.
10. Kim, S. Pittsburgh synagogue shooting: Gab, social network used by suspect, forced offline. Atlanta Journal Constitution, https://www.recordedfuture.com/dark-web-networks/, last accessed 2019/05/08.
11. Nguyen, K. Christchurch butcher Brenton Tarrant copies ISIS social media strategy: Expert. The New Daily, https://thenewdaily.com.au/news/world/2019/03/17/christchurch-butcher-brenton-tarrant-copied-isis-social-media-strategy-expert/, last accessed 2019/05/08.
12. Cowan, J. What to Know About the Poway Synagogue Shooting. The New York Times, https://www.nytimes.com/2019/04/29/us/synagogue-shooting.html, last accessed 2019/05/08.
13. Cornish, A. Places of Worship Are Increasingly becoming Targets of Extremist Violence. National Public Radio, https://www.npr.org/2019/04/29/718394039/places-of-worship-are-increasingly-becoming-targets-of-extremist-violence, last accessed 2019/05/08.