International Journal of Cyber Criminology
Vol 8 Issue 2 July - December 2014

Technological Skills of White Supremacists in an Online Forum: A Qualitative Examination

Thomas J. Holt[1] **& Micah-Sage Bolden**[2]
Michigan State University, United States of America

Abstract

Research surrounding radicalization to and use of violence among extremist and terror groups has expanded over the last decade. There are still fundamental questions that must be addressed, particularly regarding the role of the Internet in radicalization and recruitment as well as general technological skill within extremist groups. Few studies have considered this issue, especially among Far Right groups which have been identified as one of the top threats to public safety within the United States. This exploratory study addresses these issues using a qualitative analysis of a sample of threads from a technology-specific subforum of a widely used web forum in the white nationalist and white power movement. The findings demonstrate that the process of information sharing is distinct from that of more sophisticated deviant and criminal communities on-line, as users readily answer basic technological questions rather than discuss offensive attack techniques. The implications of this study for future research are examined in depth.

Keywords: Far Right, White Nationalist, Hacking, Technology, Extremist, Terror.

Introduction

The process of radicalization into extremist and terror movements has received increasing attention by scholars over the last decade, driven by the progressively prevalent threat of terroristic violence perpetrated around the world. Much of this research is driven by open source material and databased information on violent extremism, which has identified pathways that lead an extremist to violence (Bakker, 2006; Borum, 2011a, 2011b; Brenner, 2008; Freilich, Chermak, Belli, Gruenewald, & Parkin, 2013; Hafez, 2006; Hamm, 2007; Kunkle, 2012; McCauley & Moskalenco, 2011; Monohan, 2011; Sageman, 2004; Silber, 2012; Simi & Futrell, 2010; Stern, 2003).

There is, however, a limited body of research on the role of the Internet and online discourses in the radicalization process to violent ideologically-motivated activity (Brown & Douwe, 2009; Corb, 2011; Tsfati & Weimann, 2002; Weimann, 2011). There is evidence that a range of websites and on-line content are used by members of both the far right and Islamic extremist movements to promote their ideologies through mass-media

[1]Associate Professor, School of Criminal Justice, Michigan State University, 434 Baker Hall, 655 Auditorium Road, East Lansing, MI 48864, United States of America. Email: holtt@msu.edu
[2]Master's Candidate, School of Criminal Justice, Michigan State University, 434 Baker Hall, 655 Auditorium Road, East Lansing, MI 48864, United States of America. Email: boldenmi@msu.edu

(Denning, 2011; Freiburger & Crane, 2011; Holt, 2010, 2012; Jenkins, 2012; Kilger, 2011; Kunkle, 2012; Silber, 2012; Weimann, 2011). In fact, social media provides an avenue to spread news stories that may enrage individuals and lead to an acceptance of radical agendas (Corb, 2011; Kunkle, 2012). The Internet also provides an outlet to coordinate real world events across multiple areas and facilitate social relationships (Erez, Weimann, & Weisburd, 2011; Simi & Futrell, 2010). In fact, recent research suggests individuals who engaged in extremist behaviors either maintained or visited websites hosting radical group content (Chermak, Freilich, & Simone, 2010; Freilich et al., 2013; Silber, 2012).

In light of this evidence, it is important to assess how well extremist and terror groups understand and can utilize the technologies at their disposal (Gruen, 2005; McCauley, 2009; Weimann, 2011). While the Internet has a distinct role in recruitment and information sharing for terrorists, it is unclear how many members operate at a high level of technological sophistication and use the Internet for offensive attacks against on-line resources (Denning, 2011; Kilger, 2011). Though there is minimal evidence that members of the Far Right have engaged in cyber attacks against government or civilian targets, few researchers have considered why this might be the case. Cyberspace provides an unparalleled number of targets that could be affected, and done so with fewer resources than are needed to engage in physical attacks (Denning, 2011). Thus, there is a need to understand why and how members of the Far Right may discuss technology and their ability to leverage it for attacks against infrastructure or as a means to defensively anonymize their on-line identity and communications habits.

The present study seeks to address these questions through a qualitative analysis of posts made in a well-known online Far Right discussion forum in the United States. Though this movement in the US is highly segmented based on regional and religious affiliation, its members have engaged in a substantial number of violent acts in support of their beliefs (Chermak et al., 2010; Freilich et al., 2013). Furthermore, they are viewed as one of the top two threats to American public safety (Freilich et al., 2014). This movement provides an ideal group to explore the acquisition and dissemination of technology-related information on-line. In addition, this study considers the way that users express their online identity within the movement, and their use of both protective technologies and offensive cyber attack capabilities. The implications of this research for our broader understanding of the role of technology within extremist movements and future scholarship are considered in detail.

The Far Right Subculture and the Internet

In order to understand the technological capabilities of extremist movements, it is necessary to first consider the ways individuals become a part of radical social groups and the role of technology in this process. Radicalization into extremist movements has been examined by a plethora of scholars utilizing structural, psychological, social, economic, and circumstantial predictors. Most researchers agree that the process is multifaceted, and cannot be explained by any one factor (Bjorgo & Hogan, 2009; Borum, 2011a, 2011b; Horgan, 2005; Kimhi & Even, 2006; Linden & Klandermans, 2006; McCauley & Moskalenko, 2008; Taylor & Horgan 2006). One of the most influential frameworks (McCauley & Moskalenko, 2008) identifies twelve mechanisms affecting radicalization at the individual, group, and mass levels. They define radicalization as the process of "increasing extremity of beliefs, feelings, and behaviors in directions that increasingly

justify intergroup violence and demand sacrifice in defense of the ingroup" (McCauley & Moskalenko, 2008, p. 416).

Individual attitudes and experiences are critical when examining the process of radicalization into violence in support of extremist beliefs. Individuals who are emotionally vulnerable, whether because of feelings of anger, alienation, or disenfranchisement, are more likely to make the transition to morally justifying violence as an alternative to obtain political or social goals (Kimhi & Even 2006; Taylor & Horgan, 2006). Several models of radicalization identify the importance of cognitive openings, where a personal crisis or sense of longing leaves individuals receptive to new world views, as key to initiating the radicalization process (Bjorgo & Horgan, 2009; McCauley & Moskalenko, 2008; NYPD, 2007; Simi & Futrell, 2010; Taylor & Horgan, 2006; Wiktorowicz, 2004). Those who are exposed to radicalized messages during this period may be more willing to accept and justify value-systems of an extremist movement and the use of violence as a political strategy (McCauley & Moskalenko, 2008; Simi & Futrell, 2010).

Within the Far Right movement in the United States, there is a heavy emphasis on racism, conspiratorial worldviews, and the centralization of an idealized white identity (Freilich et al., 2013). This movement in the United States is highly fractured, divided among several distinct branches though the majority of research focuses on white nationalists and white power groups including the Ku Klux Klan, the Christian Identity movement, racist skinheads, neo-Nazis, and Odinists (Freilich et al., 2013; Simi & Futrell, 2006, 2010). Despite the factionalism of the movement, these branches share a core set of beliefs including a plot to exterminate the white race, a conspiratorial worldview typified by a belief in a "Zionist Occupied Government" (ZOG), the condemnation of other races and miscegenation, a belief in the inevitability of a racial holy war (RAHOWA), and a belief in some form of historical Revisionism (Bowman-Grieve, 2009). The acceptance of these beliefs leaves white nationalists on the fringes of society and culturally isolated from others (Freilich et al., 2013; Simi & Futrell, 2006, 2010). Acknowledging membership or affiliation to a white supremacist group in the real world is risky as others may respond with hatred and, in some cases, violent retribution from community members and employers (Blee, 2002; Dobratz & Shanks-Meile, 1997; Simi & Futrell, 2010)

The social stigma associated with membership in the white power movement has led the Internet has become a critical resource for members and its general persistence and growth over time (Kunkle, 2012; McCauley & Moskalenko, 2008; Simi & Futrell, 2010). The Internet acts as one of the few free spaces available to members of the white power movement where they are able to freely discuss and share their viewpoints, materials, and plans without fear of reprisal (Simi & Futrell, 2010; Weimann, 2011). In addition, individuals use the Internet as a means to identify others within their geographic location, or arrange meetings and events in the real world (Simi & Futrell, 2006, 2010). Online outlets also allow for the free distribution of white nationalist merchandise and cultural materials that would otherwise be unavailable to white nationalists, such as white power music or clothing (Lee & Leets, 2002; Levin, 2002).

Beyond the networking capability afforded by the Internet, members of the white supremacist community demonstrate their identity through the use of linguistic indicators that identify them as members of the in-group. The use of common symbols such as 88 (standing for HH, or Heil Hitler) or phrases such as the 14 Words of David Lane (Anahita, 2006; Dentice & Williams, 2010; Simi & Futrell, 2006, 2010). The use of text-based

identifiers are key since the lack of physical cues in on-line spaces require individuals to demonstrate their group affiliation and connection to the movement in more profound ways (Holt, 2010).

Though the Internet is a vital resource in the facilitation of the white supremacist movement, it is unclear how well its members either understand or can manipulate computer technology to engage in attacks against various on-line targets. Anecdotal evidence suggests that Al-Qaeda, and the so-called e-Jihad, espouse the value of cyber attacks against financial institutions and government targets (Britz, 2010; Denning, 2011, Holt, 2012). Attempts to harm the economic and communications backbone of a nation are thought to have a greater impact on the psyche of citizens and cause substantive economic harm that may be greater than what may be possible through a physical attack (Britz, 2010; Holt, 2012). A small number of successful cyber attacks have been attributed to this movement, largely involving denial of service attacks to keep others from accessing data or services, and web defacements to promote their message (e.g. Denning, 2011; Gonsalves, 2013).

By contrast, there has been few, if any, documented instances of cyber attacks attributed to the white nationalist community. It is unknown if this is due to a lack of technical capacity or acumen, or simply a lack of interest in attacks against virtual targets by members of the Far Right generally. It is likely that systemic conditions may affect the technical capabilities of the Far Right. Specifically, members of white nationalist and supremacist movements are of various ages, with some in their 50s and 60s, though the majority seem to be in their late teens to mid 30s (Anti-Defamation League, 2008; Freilich et al., 2013; Simi & Futrell, 2006, 2010). Individuals in their 50s and 60s generally report limited technology use and proficiency tend to use desktop computers rather than mobile devices, and report limited participation in social media sites (Smith, 2014).

Younger members of white nationalist groups may use the Internet with greater frequency in keeping with national trends on age-attenuated technology use (Duggan & Smith, 2013), though they may be constrained by limited access to laptop and desktop computers. This is because many white supremacist groups are located in lower income rural areas (Kunkle, 2012; McCauley & Moskalenko, 2008; Simi & Futrell, 2010). Individuals residing in these communities tend not to have a computer at home, and rely more on public libraries and mobile phones to access the Internet (Zickuhr et al., 2013). Without regular access to a computer in an unsupervised location, it may be difficult for individuals to acquire the skills necessary to engage in cyber attacks (Denning, 2011).

In addition, remote or rural residential areas tend to use dial-up Internet connectivity at home due to the difficulty in actually running broadband or cable Internet connections to these locations (Zickuhr et al., 2013). Dial-up users experience drastically slower connection speeds than modern broadband and cable modem technologies, or even some cellular service providers (Smith, 2010). This may limit the amount of time that individuals choose to spend online, which may in turn hinder the development of skills needed in order to engage in effective cyber attacks (Cooper & Harrison, 2001; Holt, 2007). Instead, members of the Far Right may turn to social media platforms and leverage the communications capabilities of the Internet through mobile devices to spread their message and recruit members.

Taken as a whole, there are various issues that may limit the cyber attack capabilities of the white nationalist movement in the US. As a result, there is a need to understand how well its participants understand and use technology to assess their proficiency and

prospective use of offensive and defensive computing resources (see also Denning, 2011). To address these issues, this study utilizes a qualitative analysis from a sample of posts from a technology-focused subforum of a well-known white supremacist forum. The data provides a more thorough exploration of the subculture and identity of participants in this movement in their own words. Additionally, the findings can demonstrate the range of technological skill among participants and their ability to employ various tools to protect themselves while on-line.

Data and Methods

The data set for this analysis consists of a set of 60 threads posted in the technology subforum of a very large web forum used by members of the white nationalist and far-right movement in the US and Europe. Web forums are a form of asynchronous on-line communication where individuals can discuss a variety of ideas or ask questions and receive responses (Holt, 2010). They are usually compartmentalized into sub-forums that center on a specific topic or issue. Each subforum is composed of threads which begin when an individual creates a post within a forum, asking a question or giving an opinion. Other people respond to the remarks with posts of their own that are connected together to create threads. In this way, threads are composed of posts that center on a specific topic under a forum's general heading.

Since posters respond to one another within and across threads, the exchanges present in a forum often resemble focus group discussions (Holt, 2007, 2010; Holt & Lampke, 2010; Mann & Sutton, 1998). This makes forum threads an ideal resource to examine relationships between individuals and gather direct detail on the issues individuals are interested in, as well as the quality and strength of ties between participants. They also include a variety of users with different skill levels and knowledge, demonstrating the range of technical proficiency within a community (Holt, 2007; Holt, 2013; Mann & Sutton, 1998).

A subforum focusing on cyber security, privacy, and encryption was selected from the large range of topics available in the larger forum to garner direct insights on the ways that users of all skill levels use and understand technology. The forum that hosts this content has a substantial user population of more than 280,000 users, with new posts made every day. In addition, this forum is publicly accessible, meaning that individuals are not required to register with the site in order to examine previous posts. Individuals who are attempting to gain entry into the extremist community as a whole are more likely to begin by identifying public, rather than private forums (Holt, 2012). Though private or registration-only forums may contain more information on how to engage in illicit activities (Holt, 2012; Holt & Lampke, 2010; Meyer, 1989) the fact that this forum is one of the most active in the Far Right suggests it is a prominent resource that individuals may turn to for information, regardless of their knowledge or involvement in the movement.

Though this data provides substantive insights into the nature of technology use within the white nationalist community, a sample of threads from a single forum does not provide a generalizable sample. There are, however, a generally limited range of forums available for members of the white nationalist community (Southern Poverty Law Center, 2014). This may stem from the substantive crackdown on on-line hate speech and Far Right groups internationally (Yar, 2013), making it difficult for groups to create or maintain long-standing on-line communities. Additionally, there is a limited focus on technology in the larger forum where this subforum was identified, despite its reputation as one of the

largest and oldest forums operating for white nationalists. In fact, only one other sub-forum was identified in this site which included topics on technology, though the topics discussed by users indicated it was unrelated to general issues regarding technological competency and use by members.

As a result, the threads included in this analysis serves as a purposive and convenient sample of user discussions focused exclusively on technology use and manipulation by member of the white nationalist subculture. Furthermore, this sample of threads involved 117 users across a 24 month period. Though this is a smaller proportion of the total registered population of over 280,000 individuals, there is no way to immediately identify how many of the total user population posts on a daily basis or actively participate in the various subforums of the site.

Despite this issue, it is clear that the threads in this sample were regularly updated with consistent, on-going conversation between users. The fact that over two years of posts were observed in a sample of only 60 threads also supports the notion that this subforum has an active user population that attempt to engage one another (Holt, 2010). Thus, this sample of threads may have limited generalizability, but provides a purposive yet convenient sample appropriate for this exploratory analysis.

The content of these threads was coded using tenets of grounded theory methodology (Corbin & Strauss, 2007). This methodology is particularly useful as its procedures permit the researcher to develop a thorough, well-integrated examination of any social phenomena. Any concepts found within the data must be identified multiple times through comparisons to identify any similarities (Corbin & Strauss, 2007). In this way, findings are validated by their repeated appearances or absences in the data, ensuring they are derived and grounded in the data. Specifically, posters repeated comments or observations regarding technology, its use, and their perceptions of government and industry were used to assess the capacity for technology use within this population. This strategy is used to structure the analysis, beginning with an examination of the types of technology discussed by users. The ways that identity is structured by participants on the basis of technology and white nationalist interests is then examined in depth using quotes from the data where appropriate. The usernames of the posters are not, however, provided in an effort to maintain some confidentiality for the sample.

Findings

Technology Use

Examining the technological component of the discussions in this subforum demonstrates that the majority of users are not technologically sophisticated. Approximately 30% of all threads (n=18) began with a user asking a question, and the majority of these questions focused on some sort of protective technology to hide an individual's location or identity. For instance, several users asked questions about the use of Tor, a free proxy service that helps to anonymize an individual's web traffic. In fact, a whole thread was dedicated to proper implementation and use of Tor in order to hide an individual's location. Such a tool is of substantive value for those in the white nationalist movement in order to conceal their risk of detection by law enforcement and intelligence agencies. In fact, one user in discussing an FBI-led takedown of a child pornography ring noted: "Keep in mind that online WN activism could potentially become illegal. Should

we congratulate the FBI finding a -loophole in Firefox and Tor when one day it will be our one safeguard?"

A number of users also asked about ways to access on-line content due to ISP-based restrictions of hate speech. For instance, one user wanted information on IP tracing to minimize his on-line footprint: "I ask because I am part of some non-racialist forums, and the thought has crossed my mind that I would most likely be immediately banned from them if it were discovered that I am a regular poster over here." While multiple responses were provided, an individual expanded on previous points by suggesting that additional steps would be necessary to help minimize their likelihood of detection and arrest. The user explained the need for encryption software to protect their hard drive and increase the difficult for law enforcement investigation:

> If you live in a country where using [the forum] might be a problem (legally) - using software like Truecrypt [an encryption program] is a good idea, however it's merely on of good practices and the last line of defense if you actually become targeted by a "thought crime" investigation, your apartment is raided and they take your computer or HDDs to search for bits and pieces of evidence (usually left on HDD from using websites). Having your HDD encrypted (with a long, well-chosen password) may help, but most people try not to actually get to the point where this happens - that's where things like VPNs & being careful about posting personal details online come into play.

A similar thread was created focusing on how Italian and European forum users could gain access to the site due to IP blocking policies. One user indicated that proxy services may not be sufficient protection, stating: "What practical advices can we give to Italian [forum users], given the circumstances? Apparently some of the recently arrested ones had tried to use proxies. There is a concern that this may not be enough"

Similarly, there was an emphasis on anonymity and tools to obfuscate a person's on-line activities. For instance, one person posted a thread asking for information on how to best secure their email, chat, Voice over IP telephony system, and search engine. A thread also focused on how Google tracking operates and how that could be reduced. Some also discussed simple techniques that could be applied to minimize one's online footprint in order to reduce the potential for identification. For instance, a user explained how law enforcement could assemble information about an individual based on their use of personal identifiers in various on-line outlets, stating:

> Antifa or police operatives can use another method [versus direct IP tracing] - reading all posts by some user on [the forum] carefully and recording all the details and clues they can find. Or putting your name into Google and finding account (sic) of similar name elsewhere if such exist or something else that is related.

Another user supported this notion, indicating: "If you mention your email or Facebook or Skype account on [this forum] - expect that it may be looked at as well or put into Google to search for even more (Especially effective can be results from Googling the person's e-mail address - if it is exposed anywhere on [here])." Thus members gave basic tips to reduce the potential for identification through the application of various techniques.

Users also appeared to use this subforum as a venue to share relevant news stories related to the use of technology, or its abuse at the hands of government agencies. There were 67 external web links provided to news stories in this sample of threads, though the majority focused on the ways that the NSA and FBI are manipulating technology to investigate various cyber crimes. The sources for these articles were technology-focused legitimate news venues such as the BBC and Ars Technica, PC World, and the Register. The utilization of mainstream news media in this subforum diverged from the usual reliance on extremist media outlets which are otherwise common among the white nationalist movement (Simi & Futrell, 2010).

While members of this subforum focused on "defensive" tools to limit the likelihood a user may be tracked or traced while on-line, there were few instances of conversations regarding "offensive" programming, malware, hacking, and cyber attack details. The most technologically sophisticated information posted in this sample was the source code for the malware Stuxnet. This extremely sophisticated malware was used by the US as part of a series of classified attacks against the programmable logic controllers used in the Natanz nuclear enrichment plant in Iran (Sanger, 2012). The Stuxnet malware was, however, extremely sophisticated and requires a solid understanding of the programming languages used in Supervisory Control and Data Acquisitions (SCADA) systems. Thus, the release of source code was more for information purposes rather than to actually foster a cyber attack by members of this subforum. In fact, the limited technological capability of users suggests it is unlikely any of the participants could actually implement this software in the wild.

As a result, this forum appears to serve as more of a "tech support" resource for users, rather than as a facilitator for offensive attack capabilities. For instance, an individual asked a question about setting up a server and client on the same system and stated "I know we have some savvy IT folks on here so I came here first." Similar comments were evident across this sample of threads, as demonstrated by an individual who asked:

> On the bottom of my P.C. right by were (sic) it gives you the time. There is well it looks like a littleback [SIC}. OK it was green all the time, now it is RED AND IT SAYS P.C. IS UNPROTECTED. Does anyone know what it means or what I should do? Please take it easy on me, I am 56 years young half blind and all of this is NEW TO ME. THANKS EVERYONE.

These sorts of questions demonstrate that individuals have varying degrees of technical proficiency, with some being quite limited based on age or experience with computers.

The majority of posters also indicated they participated in this subforum because of the participants' level of knowledge, and their willingness to help others. One user who frequently answered technical and non-technical questions indicated they were happy to help anyone, stating: "if anyone wants ACTUAL knowledge or help with network security, data protection, anonymity and obfuscation for ANY level of experience, PM or reply." Such open information sharing demonstrates that the forum provides an important avenue for information sharing and knowledge generation.

Information Sharing and Identity Formation

Though participants in this subforum sought and provided technological information, the exchanges were in no way adversarial or aggressive as noted in other technology-focused deviant subcultures on-line (Cooper & Harrison, 2001; Holt, 2007; Holt & Lampke, 2010). There were few instances of flames or criticisms of posters for not

seeking rudimentary information on their own (Holt, 2007; Jordan & Taylor, 1998; Meyer, 1989). Instead, information was provided under the auspices of assistance to their colleagues. This may be a reflection of the overarching emphasis on a white nationalist identity that unites participants and enables connections between participants. In fact, six threads were started by individuals who were paying members or "Friends" of the site, meaning they provide financial support to maintain the site and its role in the white nationalist movement. Interestingly, all of these posts were direct requests for information and technological assistance. The questions were relatively basic and involved browser selection and the ways to use anonymizing software, suggesting they had limited technological capacity. For instance, one individual asked:

> A friend has moved into an apartment complex that has free Wifi. He cannot really afford to pay for internet access so he is thinking about using their free service. What he is worried about is can the network admin see which pages he views and if so, is there any way to stop this from happening?

This question was not met with derision or chiding, but rather led to simple responses regarding how the individual can protect themselves and find ways to anonymize or obfuscate their web traffic. As such, the process of information sharing in this subforum appears to be inclusive rather than adversarial.

Though technical questions and information were commonly posted in the forum, users did not typically infuse their comments with overt expressions of their white nationalist identities. Instead, individual philosophies and demonstrations of sub cultural commitment could be inferred through users' avatars, usernames, and signatures. For instance, the numbers 14 and 88 (representing the '14 Words' and 'Heil Hitler' respectively) were found in several usernames. Avatars were also an important outlet though which users expressed their white nationalist ideology. The most common images used included the Swastika, the Celtic Cross, the Black Sun, as well as user-generated artwork incorporating these images.

Posters could also use a signature, or individualized block of text and images that would automatically appear at the end of each post, to express their identity. Many posters included quotes from well-known racist figures such as Adolf Hitler, Joseph Goebbels, or George Lincoln Rockwell as their signatures, or included phrases that invoked white nationalist. For example, one user's signature read: "When White men start making the laws again, I'll be a law abiding citizen. Until then I'll do as I damned well please."

User posts also contained minimal use of common slang terms or concerns otherwise discussed by members of the white nationalist movement. There were only two instances of individuals using the term ZOG, one of which was used in the context of a discussion regarding the hacker collective Anonymous and the use of connectivity tools to obfuscate a user's location. The user indicated:

> Some of the hacktivists are using Anonymous VPN. As most people probably know, Anonymous are the hacktivist group some of who, both knowingly and some unknowingly, hack for ZOG. If you are downloading torrents [engaging in digital piracy] or doing something relatively innocuous then you could [use this VPN] to hide amongst their crowd... I would NOT use that service to visit WN sites or to do any sort of business, but...this is one of the countless options.

Similarly, there were very few posts generally denigrating other races and ethnic groups. The only substantive comments in this regard were posted about the Apple corporation, as in this quote from one of the forum users: "No WN should ever own a Dell or an Apple computer. Steve Jobs was an Arab who took a blonde woman. To this day, Apple is the company of leftists and multiculturalists."

One of the most unique threads linking both technology and white nationalist identity together was a post by two users who were working together to create a variant of the open-source operating system software Linux. The creators called this build "Apartheid" in reference to the government sanctioned segregation of whites and blacks in South Africa, and indicated it was "Linux for proud whites." The developers explained their rationale for its creation stating:

> Built on PCLinux OS LXDE edition, Apartheid comes with Tor enabled and working out of the box, allowing you to surf the web anonymously and much safer than using a regular proxy. In addition to full multimedia support and custom artwork, it uses the lightweight LXDE desktop environment. This makes it fast and well suited as a live cd OS for those who want to get speed out of their computers while preserving ease of use and keeping oppressive governments at bay.

They requested that members of the subforum download the operating system and provide feedback as to how to improve the program or any additional resources that may benefit the user. A number of posters responded with comments as with these two posts:

> **User 1**: It runs pretty smoothly, even boots faster than Debain! Plus I love the fact that all the dvd & mp3/mp4 codecs are installed, unlike allot other distros! But I not a fan of the triskele/swastika logo cause its been vilified so much by the jews. I suggest changing it to a more universally clean and accepted White symbol for the logo such as Aryan fist, Celtic Cross, German Cross or the Life Rune. Cause I believe this operating system can be excellent tool for waking people up, but having a swastika logo will turn off some unawakened whites or Whites Nationalist that are not National Socialist.

> **User 2:** I got Apartheid installed & running flawlessly on VirtualBox with a Linux Mint host! I also going try it on Microsoft Virtual PC 2007 with a XP SP3 host tomorrow, I will post my results from that.
> Here's 2 more suggestions for the login,
> 1. The blue hover highlight makes the blue text almost impossible to read. I suggest hover text to be white with the blue hover highlight.
> 2. The bold and increase the font on the date & time for readability.

It is important to note that individuals who responded to the post regarding Apartheid appeared to be more technically proficient, and also committed to a white nationalist identity. These users divulged that they worked in either information security or technology support fields, and even had some connection to the larger hacker subculture. For instance, one user indicated he was involved in both the hacker and white nationalist subcultures:

> [I have] Been to 5 defcons [the largest hacker convention in the US], had 13 separate publishings [SIC] in 2600 [a quarterly magazine published for the hacker

> community] under the same handle and find myself rather isolated in my state. Even though it is the WHITEST in the entire union.

This quote illustrates that individuals who are involved in both IT-focused jobs and are ideologically aligned with the white nationalist movement may feel extreme social isolation. Being able to actively contribute to the knowledge development of others in the movement may reduce their sense of separation and engender a better sense of community around issues of interest to the white nationalist sub cultural identity.

Discussion and Conclusion

This study sought to understand the extent to which the online white supremacist community discussed and utilized computers and the Internet, and their capacity for cyber attacks generally. The findings suggest that a small proportion of posters may have sophisticated technological backgrounds relative to the wider audience of forum users (see also Holt, 2007). Instead, most users demonstrate a basic degree of technological proficiency, making it clear that they came to this subforum in order to gain insights. Additionally, most discussions centered on tools that could hide an individual's location and information from outsiders and law enforcement. In fact, the majority of conversations involved the use of Tor and software programs to anonymize individual on-line behavior. This is sensible given the pervasive belief among members of this movement that they are being tracked and pursued by government agents and law enforcement (Freilich et al., 2013; Simi & Futrell, 2010). Thus, keeping up to date on news stories involving government investigations on-line and developing knowledge of how to hide one's identity fits with the larger norms of the Far Right subculture (Bowman-Grieve, 2009; Freilich et al., 2013; Simi & Futrell, 2010).

Since a small number of forum users had demonstrable technical skill, they act as a key resource for the broader population of unskilled users. These individuals provide substantive information without being combative or challenging others, and in quick, easy-to-digest bits with minimal prompting or re-posting. This process is dramatically different from other information sharing processes observed in criminal subcultures on-line (Cooper & Harrison, 2001; Holt, 2007; Jordan & Taylor, 1998). Research suggests technologically-focused subcultures emphasize outward demonstrations of knowledge or expertise prior to giving any assistance, and may be aggressive with one another on-line (Holt, 2007; Meyer, 1989).

As a result, white nationalists' on-line communication patterns may be reflective of an attempt to ingratiate individuals and foster a community rather than aggressively demonstrate technological skill. It is also important to note that this forum was populated by individuals who offered financial support to keep the site operating. Such an individual is likely to be either older or more heavily entrenched in this movement, and their involvement in this technology-specific subforum creates a unique point of entry and potential for acceptance of radical ideologies. Specifically, socially isolated individuals may be more likely to accept and engage in extremist movements, particularly in on-line communities. The ability to share one's technical knowledge and gain status within the forum may lead that user to feel more socially accepted and incorporated into the community (Bjorgo & Horgan, 2009; McCauley & Moskalenko 2008; Simi & Futrell, 2010; Wiktorowicz, 2004).

It is unclear if this may lead an individual to engage in some form of cyber attack or real world violence over time, though it does seem to fit into some part of the

radicalization process (McCauley & Moskalenko, 2008). Greater research is needed to examine the pathway that lead individuals to cyber attacks rather than real world violence in extremist movements, and identify any commonalities between these processes (see also Holt & Kilger, 2012; Kilger, 2011).

Additional research is also needed with larger forum samples to better assess the composition of technological skill among the members of the Far Right, and the Islamic extremist community generally. Though there was only one technology-focused subforum within this site, its participants may not be representative of the larger population of forum users, or the larger universe of Far Right groups generally. Gathering a larger sample of threads from multiple forums is necessary to replicate the findings of this study, and identify variations in the distribution of skill. Collecting data in more underground, registration-controlled forums may also demonstrate variations in the interests of users and potential insights on offensive attack details which may otherwise be absent from publicly accessible forum content (see Holt, 2010). Comparing forum posts against social media feeds such as Twitter and Facebook would also give substantive insights into the ways that members of the Far Right utilize technology for different purposes (see also Erez et al., 2011; Simi & Futrell, 2010).

Similarly, quantitative surveys of the technological skill and awareness of members of white supremacist groups would be invaluable to measure the technological expertise of the Far Right. Such a process would, however, be inherently difficult due to the general mistrust of researchers among members of this subculture (see Blee, 2002; Dobratz & Shanks-Meile, 1997; Simi & Futrell, 2010). Thus, researchers must find alternative points of data collection so as to improve our access to and understanding of the white supremacist movement and the nature of the threat posed by extremist groups on-line. Furthermore, these studies can improve our knowledge of the overlap and intersections between on-line subcultures with different interests and information sharing processes (see Holt, 2007, 2010).

References

Anahita, S. (2006). Blogging the Borders: Virtual Skinheads, Hypermasculinity, and Heteronormativity. *Journal of Political and Military Sociology, 34,* 143-164.

Anti-Defamation League. (2008). *American Stormtroopers: Inside the National Socialist Movement.* New York, NY: Anti-Defamation League. Retrieved on 13th March 2014 from http://archive.adl.org/learn/ext_us/nsm/nsm_reportv12.pdf

Bakker, E. (2006). Repression, Political Violence and Terrorism. The Case of Uzbekistan. *Helsinki Monitor: Security and Human Rights*, *17*, 108-118.

Bjorgo, T. & Horgan, J. (2009). *Leaving Terrorism Behind: Individual and Collective Disengagement.* Oxon: Routledge.

Blee, K. M. (2002). Inside *Organized Racism: Women in the Hate Movement.* Berkley, CA: University of California Press.

Borum, R. (2011a). Radicalization into violent extremism I: a review of social science theories. *Journal of Strategic Security, 4*, 7-36.

Borum, R. (2011b). Radicalization into violent extremism II: a review of conceptual models and empirical research. *Journal of Strategic Security, 4,* 37-62.

Bowman-Grieve, L. (2009). Exploring "Stormfront": A Virtual Community of the Radical Right. *Studies in Conflict and Terrorism, 32,* 989-1007.

Brenner, W. J. (2008). Confounding powers: Dominance and discord in international politics from the assassins to Al Qaeda. The John Hopkins University, ProQuest, UMI Dissertations Publishing.

Britz, M. T. (2010). Terrorism and technology: Operationalizing cyberterrorism and identifying concepts. In T. J. Holt (Ed.), *Crime On-Line: Correlates, Causes, and Context* (193-220). Raleigh, NC: Carolina Academic Press.

Brown, I., & Douwe, K. (2009).Terrorism and the Proportionality of Internet Surveillance. *European Journal of Criminology*, *6,* 119-134.

Chermak, S. M., Freilich, J. D., & Simone, J. (2010). Surveying American state police agencies about lone wolves, far-right criminality, and far-right and Islamic jihadist criminal collaboration. *Studies in Conflict and Terrorism, 33,* 1019-1041.

Chu, B., Holt, T. J., & Ahn, G. J. (2010). *Examining the Creation, Distribution, and Function of Malware On-Line.* Technical Report for National Institute of Justice. NIJ Grant No. 2007-IJ-CX-0018.

Cooper, J., & Harrison, D. M. (2001). The social organization of audio piracy on the Internet. *Media, Culture, and Society*, *23*, 71-89.

Corb, A. (2011). *Into the minds of mayhem: White supremacy, recruitment and the Internet.* A report commissioned for Google Ideas.

Corbin, J. & Stauss, A. (2007). *Basics of Doing Qualitative Research: Techniques and Procedures for Developing Grounded Theory.* Thousand Oaks, CA: Sage.

Denning, D. E. (2011). Cyber-conflict as an Emergent Social Problem. In T. J. Holt & B. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*. Hershey, PA: IGI-Global.

Dentice, D. & Williams, J. L. (2010). The First 100 Days: Stormfront Responds to Obama's Presidency. *Theory in Action,* 3.

Duggan, M., & Smith. A. (2013). *Social Media Update: Demographics of Key Social Networking Platforms*. Pew Research Internet Project. Retrieved on 20th November 2014 from http://www.pewinternet.org/2013/12/30/demographics-of-key-social-networking-platforms.

Freilich, J. D., Chermak, S. M., Belli, R., Gruenewald, J., & Parkin, W. S. (2013). Introducing the United States Extremist Crime Database (ECDB). *Terrorism and Political Violence, 25,* 1-13.

Freiburger, T., & Crane, J. S. (2011). The Internet as a terrorist's tool: A social learning perspective. In K. Jaishankar (Ed.), *Cyber criminology: Exploring Internet crimes and criminal behavior.* (127-138). CRC Press: Boca Raton, FL.

Gonsalves, A. (2013). Islamic group promises to resume U.S. bank cyber attacks. *CSO Online* February 28, 2013. Retrieved on 24th January 2014 from: http://www.csoonline.com/article/729598/islamic-group-promises-to-resume-u.s.-bank-cyberattacks?source=ctwartcso.

Hafez, M. M. (2006). Suicide Terrorism in Iraq: A Preliminary Assessment of the Quantitative Data and Documentary Evidence. *Studies in Conflict and Terrorism, 29,* 591.

Hamm, M. S. (2007). *Terrorism As Crime: From Oklahoma City to Al-Qaeda*. New York: NYU Press.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Journal of Deviant Behavior, 28,* 171-198.

Holt, T. J. (2010). Exploring strategies for qualitative criminological and criminal justice inquiry using on-line data. *Journal of Criminal Justice Education, 21,* 300-321.

Holt, T. J. (2012). Exploring the intersections of technology, crime and terror. *Terrorism and Political Violence, 24,* 337-354.

Holt, T. J. (2013). Exploring the social organization and structure of stolen data markets. *GC, 2,* 155-174.

Holt, T. J. & Lampke, E. (2010). Exploring stolen data markets on-line: Products and market forces. *Criminal Justice Studies, 23,* 33-50.

Holt, T. J., & Kilger, M. (2012). Examining Willingness to Attack Critical Infrastructure Online and Offline. *Crime & Delinquency, 58,* 798-822.

Horgan, J. (2005). *Psychology of Terrorism.* New York: Routledge.

Jordan, T. & Taylor, P. (1998). A Sociology of Hackers. *The Sociological Review, 46,* 757-780.

Kilger, M. (2011). Social dynamics and the future of technology-driven crime. In T. J. Holt & B. Schell (Eds.) *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (205-227). Hershey, PA: IGI-Global.

Kimhi, S. & Even, S. (2006). The Palestinian Human Bombers. In J. Victoroff (Ed.) *Tangled Roots: Social and Psychological Factors in Genesis of Terrorism* (308-323). Washington, D.C.: IOS Press.

Krueger, A. B. (2007). *What Makes a Terrorist: Economics and Roots of Terrorism.* Princeton and Oxford: Princeton University Press.

Kunkle, J. (2012). Social Media and the Homegrown Terrorist Threat. *The Police Chief, 79,* 22.

Lee, E., & Leets, L. (2002). Persuasive storytelling by hate groups online: Examining its effects on adolescents. *American Behavioral Scientist, 45, 927-988.*

Levin, B. Cyberhate: A legal and historical analysis of extremists' use of computer networks in America. *American Behavioral Scientist, 45,* 958-988.

Linden, A. & Klandermans, B. (2006). Stigmatization and Repression of Extreme-Right Activism in the Netherlands. *Mobilization: An International Journal, 11,* 213-228.

Mann, D. & Sutton, M. (1998). Netcrime: More Change in the Organization of Thieving. *British Journal of Criminology, 38,* 201-229.

McCauley, C. & Moskalenko, S. (2008). Mechanisms of Political Radicalization: Pathways Toward Terrorism. *Terrorism and Political Violence, 20,* 415-433.

McCauley, C. & Moskalenko, S. (2011). *Friction: How radicalization happens to them and us.* New York City: Oxford University Press.

Meyer, G. R. (1989). The Social Organization of the Computer Underground. Unpublished Masters Thesis. Retrieved on 20th January 2014 from http://csrc.nist.gov/secpubs/hacker.txt.

Monohan, J. (2012). The Individual risk assessment of terrorism. *Psychology, Public Policy and Law.* In Press.

NYPD. (2007). Radicalization in the West: The Homegrown Threat. New York.

Sageman, M. *Understanding Terror Networks.* Philadelphia: University of Pennsylvania Press.

Schell, B. H. & Dodge, J. L. (2002). *The Hacking of America: Who's Doing it, Why, and How.* Westport, CT: Quorum Books.

Silber, M. D. (2012). *The Al Qaeda factor: plots against the West.* Philadelphia: University of Pennsylvania Press.

Simi, P. & Futrell, R. (2006). Cyberculture and the Endurance of White Power Activism. *Journal of Political and Military Sociology, 34,* 115-142.

Simi, P. & Futrell, R. (2010). *American Swastika: Inside the White Power Movement's Hidden Spaces of Hate.* New York: Rowman and Littlefield Publishers, Inc.

Smith, A. (2010). *Home broadband 2010.* Pew Internet and American Life Project. Retrieved on 11th January 2014 from http://pewinternet.org/Reports/2010/Home-Broadband-2010.aspx.

Smith, A. (2014). *Older adults and technology use.* Pew Internet and American Life Project. Retrieved on 11th January 2014 from http://www.pewinternet.org/files/2014/04/PIP_Seniors-and-Tech-Use_040314.pdf.

Southern Poverty Law Center. (2014). *White Homicide Worldwide.* Retrieved from http://www.splcenter.org/get-informed/publications/White-Homicide-Worldwide

Stern, J. (2003). Terror in the name of God. *Terrorism and Political Violence, 15,* 190-201.

Taylor, M. & Horgan, J. (2006). A Conceptual Framework for Addressing Psychological Process in the Development of a Terrorist. *Terrorism and Political Violence, 18,* 585-601.

Taylor, P. A. (1999). *Hackers: crime in the digital sublime.* New York: Routledge.

Thomas, D. (2002). *Hacker Culture.* Minneapolis, MN: University of Minnesota Press.

Wiktorozicz, Q. (2004). *Joining the Cause: Al-Muhajiroun and Radical Islam.* The Roots of Radial Islam. Department of International Studies, Rhodes College.

Yar, M. (2013). *Cybercrime and Society.* Thousand Oaks, CA: SAGE.

Zichuhr, K., Rainie, J., Purcell, K., & Duggan, M. (2013). *How Americans value public libraries in their communities.* Pew Internet and American Life Project. Retrieved on 11th January 2014 from http://libraries.pewinternet.org/files/legacy-pdf/PIP_Libraries%20in%20communities.pdf.