



# Criminal Justice Studies

A Critical Journal of Crime, Law and Society

ISSN: 1478-601X (Print) 1478-6028 (Online) Journal homepage: [www.tandfonline.com/journals/gjup20](http://www.tandfonline.com/journals/gjup20)

## Extremism on the World Wide Web: a research review

W. Chris Hale

To cite this article: W. Chris Hale (2012) Extremism on the World Wide Web: a research review, Criminal Justice Studies, 25:4, 343-356, DOI: [10.1080/1478601X.2012.704723](https://doi.org/10.1080/1478601X.2012.704723)

To link to this article: <https://doi.org/10.1080/1478601X.2012.704723>



Published online: 10 Jul 2012.



Submit your article to this journal [↗](#)



Article views: 2272



View related articles [↗](#)



Citing articles: 17 View citing articles [↗](#)

## Extremism on the World Wide Web: a research review

W. Chris Hale\*

*Louisiana State University in Shreveport, One University Place, Shreveport, LA 71115, USA*

The following paper addresses the importance of the Internet in supporting rightwing extremist objectives. More specifically, this paper will examine Internet facilitation of information sharing, fundraising, social networking and recruitment, publicity, and risk mitigation. Specific tactics under investigation include, but are not limited to, the use and creation of electronic bulletin boards, the widespread adoption of multimedia technologies to attract children and teenagers, and the ever increasing use of writing and speaking in code. Given recent growth trends concerning group membership, it is imperative that Internet usage by these groups be exploited for research and intelligence purposes.

**Keywords:** extremists; white supremacists; hate groups; Internet; web-based technologies; social networking and recruitment

Responding to an early 911 call on 4 April 2009, two Pittsburgh police officers were fatally shot in the head by a gunman wearing a bulletproof vest. Lying in wait, Richard Poplawski, then murdered a third officer, igniting a four hour gun battle with Special Weapons and Tactics teams. Fueled by racism and a fear that the Obama administration was planning to facilitate right-infringing gun legislation, the officers were the first Pittsburgh city officers to die in the line of duty in 18 years (Plushnick-Masti & Nephin, 2009). Two months later, on 10 June 2009, James W. Von Brunn, a white supremacist, walked into the crowded US Holocaust Memorial Museum in Washington, DC, and immediately opened fire. Utilizing a .22-caliber rifle, Von Brunn shot and killed Stephen Tyrone Jones, one of the museum security guards. Von Brunn was a known anti-Semitic and Holocaust denier (Berger, 2009). These events, coupled with the foiled 2008 Obama assassination attempt by two neo-Nazi skinheads, point to an escalation of rightwing extremist violence, not seen since the 1990s (Simi, 2010). In fact, despite the very real threat from foreign terrorist organizations since the 11 September 2001 terrorist attacks, 'lone wolves and small terrorist cells embracing violent rightwing extremist ideology are the most dangerous domestic terrorism threat in the United States' (Department of Homeland Security (DHS)/Office of Intelligence and Analysis, 2009, p. 7).

According to Martin (2011), extremism 'is characterized by intolerance toward opposing interests and divergent opinions and is the primary catalyst and motivation for terrorist behavior' (p. 4). Further arguing that those who cross the line from

---

\*Email: [chale@lsus.edu](mailto:chale@lsus.edu)

extremism to terrorism ‘always develop noble arguments to rationalize and justify their acts of violence toward nations, people, religions, or other interests’ (p. 4). In other words, extremism should be thought of as a precursor to terrorism, often utilized to motivate and justify acts of terror. Acting as a foundation of terrorism, extremism, particularly rightwing domestic extremism, is the focus of this paper.

Utilizing the DHS/Office of Intelligence and Analysis (2009) definition:

Rightwing extremism in the United States can be broadly divided into those groups, movements, and adherents that are primarily hate-oriented (based on hatred of particular religious, racial or ethnic groups), and those that are mainly antigovernment, rejecting federal authority in favor of state or local authority, or rejecting government authority entirely. (p. 2)

Furthermore, most scholars attribute this apparent rise in rightwing extremist violence to several emergent issues (Jenkins, 2003; Simi, 2010). These issues include the current economic downturn, the immigration debate, international conflict resulting in two wars, and the election of the first African-American President. First, by exploiting the economic downturn and loss of jobs, violent rightwing extremist leaders may be recruiting new members by simply giving them someone to blame. Acting as perceived sources of economic competition, hatred, and violence against immigrants is touted as the only justifiable response. Similarly, rightwing extremists argue that the perceived rise in the number of illegal immigrants is simply a plot to destroy white America. The National Socialist Movement (NSM) in particular has focused extensively on illegal immigration for recruitment efforts (Simi, 2010). Third, rightwing extremists argue that the wars in Iraq and Afghanistan were orchestrated and fought for Jewish interests. Discussions of this issue fill white supremacist social networking sites (Simi, 2010) and are utilized to recruit US soldiers into the movement (Federal Bureau of Investigation, 2008). Finally, the election of the first African-American President has infuriated many rightwing extremists. Many of them see Barak Obama’s election as a forced infusion of non-white values and thus a threat to ‘traditional’ American culture. Fueled in large part by the Internet and social networking technologies, extremists exploit the above issues, spread propaganda, and recruit new members, ‘all of which may be contributing to the pronounced state of radicalization inside the United States’ (Federal Bureau of Investigation, 2010).

Extremists use the Internet for a variety of reasons including easy access, limited or no regulations (i.e. lack of government control), huge audiences, anonymity of communication with like-minded individuals, a multimedia environment (i.e. combination of text, graphics, audio, and video), and the ability to shape traditional mass media coverage. Information placed on the Internet by extremist groups include history and organizational activities, biographies of leaders, founders, and heroes, up-to-date news, training manuals, and fundraising activities (Weimann, 2004). Moreover, it is difficult to ascertain an accurate number of extremist groups operating on the Internet. Weimann (2006) argues that there are approximately 5000 websites supporting extremist objectives in operation today. With other researchers tending to agree (Ariza, 2006; Kaplan, 2006), these numbers represent an almost 400-fold increase in extremist websites in just 10 years. Even more disturbing and central to the present study concerns a report just released by the Simon Wiesenthal Center (2011) which suggests that there are close to 14,000 social networking sites,

forums, twitter, blogs, newsgroups, and other on demand video sites supporting just hate-motivated extremist groups alone. With only one such website<sup>1</sup> thought to be operating in 1995, hate-motivated extremist groups appear to be exploiting information and communication technologies at an increasingly alarming rate.

The following paper addresses the importance of the Internet in supporting domestic rightwing extremist objectives. Focusing primarily on white supremacist groups, this paper will examine Internet facilitation of information sharing, fundraising, social networking and recruitment, publicity, and risk mitigation. However, before addressing these concepts, a general discussion of the white power movement is warranted.

### **The white power movement**

The white power movement is essentially drawn from a network of overlapping groups, including the Ku Klux Klan, Aryan skinheads, neo-Nazis, and Christian Identity groups (Bostdorff, 2004; Kleg, 1993; Simi & Futrell, 2006a; Southern Poverty Law Center (SPLC), 2011). Representing one of the oldest and most infamous groups, the Ku Klux Klan was organized in the south following the Civil War. Although they primarily target black Americans, the Klan now targets Jews, immigrants, and homosexuals. Klan membership is estimated to be between 5000 and 8000 members. Neo-Nazi groups, on the other hand, seek to revive Nazism and hatred of Jews. This post-World War II ideology argues that Jews control government, financial institutions, and the media. Racist Skinheads are typically young, violent, have shaved heads, and participate in many types of racist events, including neo-Nazi rallies, Holocaust denial conferences, and white power music events. According to the Anti-Defamation League (2007a), Racist Skinhead membership has grown from 5000 members to 10,000 members in just six years (2001–2007). Finally, Christian Identity groups believe they are the true children of God. They believe that non-whites are soulless and Jews are ascended from Satan. Although differences exist among them, all agree on certain fundamental doctrines, including a commitment to defending the white race, the creation of a racially exclusive world where non-whites are subordinate to whites, fear of Jewish governmental domination, and opposition to homosexuality and interracial sex and marriage.

In fact, a recent study analyzing organizational mission statements from six leading white supremacist groups found that several similarities existed between the Ku Klux Klan and neo-Nazi groups (Adams & Roscigno, 2005). Pushing a victimization agenda, principal concerns included a fear that whites are becoming a numerical minority and a fear that whites are losing social authority and power. More specifically, Klan rhetoric focused on perceived legal sanctions against whites (e.g. affirmative action), perceived attacks on Christian values (e.g. homosexuals), and immigration (e.g. job loss). Neo-Nazi discourse, on the other hand, focused on cultural, social, and biological degradation, as well as, an illegitimate and oppressive Jewish government. Primary causes for these concerns included liberalism, multiculturalism, and pluralism, resulting in special treatment for minorities, political disempowerment and/or Jewish domination. Finally, whereas both argue that racial separation and segregation are the only viable options, Klan actions include more government participation, while neo-Nazi rhetoric called for a holistic restructuring of the state through ‘lone wolf’ violent action. Indeed, Perry (2000) argues

that hate groups are fully prepared to defend themselves, and in some cases, bring about a racial holy war; in that groups train in pseudo-military encampments, equipped with antitank weapons, ammunition, night vision equipment, automatic weapons, and explosives. This is not surprising, given that boundaries between white supremacists and militia groups are becoming increasingly blurred (Dees, 1996; Ridgeway, 1995).

In general, the number of hate groups operating in the USA is difficult to ascertain. Estimates have ranged anywhere from 25 (Ridgeway, 1995) to 350 (Bullard, 1991) major hate groups. Feagin and Vera (1995) estimate that there are nearly 30,000 active white supremacist members and more than 150,000 'armchair' racists. Armchair racists are those who browse websites and receive literature, but would not necessarily attend racist events or rallies. More recent estimates include research conducted by the SPLC (2011) which counted more than 1000 hate groups in 2010, a 66% rise since 2000. More specifically, the SPLC follows the activities of antigay, anti-immigrant, anti-Muslim, black separatists, Christian identity, holocaust denial, Ku Klux Klan, neo-confederate, Neo-Nazi, racist music, racist skinhead, radical traditional Catholicism, sovereign citizen, and white nationalist groups. With most, if not all such groups using the Internet to spread messages of hate and violence, the following examines Internet facilitation of information sharing, fundraising, social networking and recruitment, publicity, and risk mitigation.

## Methodology

Despite concerns from Homeland Security officials about rightwing extremist violence (see DHS/Office of Intelligence and Analysis, 2009), most research conducted since the 11 September 2001 attacks, has primarily focused on radical Islamic terrorism. This neglect has resulted in a 'significant limitation to the field of terrorism research' (Simi, 2010, p. 252). Likewise, a recent White House Terrorism Strategy (2011, p. 2) argues that 'Our threat environment is constantly evolving, which is why we must consistently revisit our priorities and ensure our domestic approach can address multiple types of violent extremism'. This manuscript not only adds to a very limited body of knowledge, but provides a comprehensive overview of how domestic rightwing extremist groups exploit the Internet.

To comprehensively assess the use of the Internet among rightwing extremist groups, a number of leading electronic databases were searched for any studies published between 1995 and 2011, addressing extremist use of the Internet. This date range was chosen, because *Stormfront.org*, the first major hate site on the Internet, was launched in 1995. The databases included Criminal Justice Abstracts with full text, SocINDEX with full text, Academic Search Complete, PsycINFO, Psychology and Behavioral Sciences Collection, and Lexis-Nexis Academic (legal). The search looked for any mention in the title, the abstract, or the keyword list of the words 'extremism', 'extremist', 'rightwing', 'hate', or 'white supremacist', with any of the following terms: Internet, web-based technologies, information sharing, fundraising, social networking, web 2.0, recruitment, publicity, and risk mitigation. All article abstracts retrieved were scanned to identify those studies that focused on 'rightwing extremist use of the Internet', as opposed to those that focused on other forms of extremism (i.e. leftwing, Islamic fundamentalism, and/or ecoterrorism, etc.). After which, the author attempted to obtain full-text copies of each article. Those not

available in full-text and/or not available on the university library shelves were obtained through interlibrary loan. Additional articles were located and retrieved from citations in the originally retrieved studies when appropriate. Also, any government documents addressing Internet extremism were located. Finally, based upon the major themes discussed in the literature, all articles were divided into the following categories: information sharing, fundraising, social networking and recruitment, publicity, and risk mitigation.

## Use of the Internet to support extremist objectives

### *Information sharing*

Prior to the advent of the Internet, white supremacist groups spread their message of hate by placing fliers under windshield wipers and/or distributing books, newspapers, magazines, and newsletters (Stern, 1999). Although somewhat effective, these methods only allowed one to reach small audiences. As technology improved, hate groups began experimenting with videotapes, fax machines, 'dial-a-hate' hotlines, and AM radio programs. Although all still utilized today, the Internet has made dissemination of hate materials quicker and more cost effective. In other words, users can instantly download (and disseminate) fliers, books, magazines and newsletters, as well as, watch and listen to recorded or live streaming audio and video in the privacy of their own homes. This is especially important given that membership in white power groups is risky, given that public rallies often draw unwanted attention and counterprotests. In addition, revelation of Aryan ideals may result in anger and isolation from employees, neighbors, and friends (Simi & Futrell, 2006b).

One such book, now widely available on every major hate site, is the *Turner Diaries* written by William Pierce (Macdonald, 1978). Representing the key work in the white supremacist movement, the *Turner Diaries* presents a fictional account detailing the violent overthrow of the government, eventually resulting in the systematic killing of Jews and nonwhites in an attempt to establish an Aryan world. Also popular among far-right extremists, a copy of the *Turner Diaries* was found in Timothy McVeigh's car following the Oklahoma City bombing. In fact, some believe that the Pierce's words inspired and provided a model for McVeigh's actions, in that a similar bomb was constructed in an attack against a federal building in the book. Pierce followed the *Turner Diaries* with another popular book among white supremacists titled *Hunter* (Macdonald, 1989). This book depicts a fictional story of a drive-by killer who assassinates interracial couples and Jews in order to racially cleanse America.

Still other sites offer organizational operational manuals. For example, Blood & Honour (racist skinhead group) offers for download their field manual<sup>2</sup> with chapters discussing ideology, organization, propaganda, violence and terror, and activist tips. Similarly, Combat 18 (also a racist skinhead group) publishes on their website, a *Combat 18 Guide to ZOG Oppression*.<sup>3</sup> This manual discusses tips on how to avoid forensic traces, such as fingerprints, glass, hair, and blood. In addition, some sites offer survivalist tips and US military training manuals, including the *US Army Infantry Rifle Platoon and Squad Manual* and the *Crew-Served Machine Gun Manual*.<sup>4</sup> Finally, other information widely available include numerous tutorials on building bombs, firing weapons, physical fitness training, plotting assassinations, and how to organize and manage an extremist cell.



### ***Fundraising***

In general, extremist groups rely heavily on donations (Conway, 2005). These donations are either directly solicited via organizational websites or indirectly through front organizations and/or charities. Money is directly solicited through credit card payment options, with many providing bank account numbers as to where money can be deposited. Some groups have even begun to profile site visitors, gathering user demographics, and then contacting those that appear to be potential supporters. Many websites offer online stores, where money is raised through the sale of books, audio and video tapes, flags, and t-shirts.<sup>5</sup>

### ***Social networking and recruitment***

Similar to tactics used to raise funds, the Internet has also proven to be an effective recruitment tool. One method utilizes recruiters who roam public online chat rooms, post messages on electronic bulletin boards, and track website user demographics in attempt to find supporters (Weimann, 2004). Once potential recruits are located, members flood them with religious decrees, training manuals, and anti-American propaganda, with much of it being audience and language specific (Thomas, 2003; Zhou, Qin, Lai, Reid, & Chen, 2006).

Often referred to as Web 2.0, social media sites, including web forums, blogs, wikis, and media-sharing websites, contain massive volumes of user-generated content (Cho & Tomkins, 2007) and have become more popular than ever (Rainie, Purcell, Goulet, & Hampton, 2011). Americans alone spend nearly one-quarter of their time online visiting social networking and blogging websites (Paul, 2011). Facebook, a top social media destination, boasts more than 800 million users (Facebook, 2011). Unfortunately, a recent White House terrorism strategy reports that many of these popular social media sites play an important role in 'advancing violent extremist narratives' (White House Terrorism Strategy, 2011, p. 6). In fact, with little or no editorial control and an environment where all users are equal participants, social networking sites allow hate and violent rhetoric to flow unchallenged (Yang, Kiang, Ku, Chiu, & Li, 2011). Research conducted by the Simon Wiesenthal Center (2009) found that many extremist groups take advantage of Facebook, including, but not limited to, Stormfront, National Socialist Life, Libertarian National Social Movement, Aryan Guard, and numerous anti-Israel organizations.

Understanding the danger of harmful content, Facebook employs a team of professionals that hunt and remove content in violation of their policies. Content removed includes actionable threats, hateful material, and nudity and/or pornography (Dodds, 2011). Nevertheless, with more than 900 million objects interacted with daily (pages, groups, events, and community pages) removing extremist content is difficult at best. Understanding the growing use of social media among violent extremist groups, the UK Home Office announced in 2009 that they would begin monitoring all conversations on social networking sites. The sites included Facebook, MySpace, Bebo, Twitter, and Skype (Espiner, 2009). More recently, US DHS Secretary Janet Napolitano stated that 'fighting homegrown terrorism by monitoring Internet communications is a civil liberties trade off the U.S. government must make to beef up national security'. Napolitano further argued that 'the First Amendment protects radical opinions, but we need the legal tools to do things like monitor the recruitment of terrorists via the Internet' (Associated Press, 2010).

In fact, in 2010, the DHS launched the Publicly Available Social Media Monitoring and Situational Awareness Initiative. This program operated by the National Operations Center (NOC) under the Office of Operations Coordination and Planning as part of the DHS, monitors numerous social media services (without any direct interaction), and subsequently, acquiring and storing publicly available information. Moreover, information is being collected

to provide situational awareness and establish a common operating picture for the entire federal government, and for state, local, and tribal governments as appropriate, in the event of a natural disaster, act of terrorism, or other manmade disaster; and ensure that critical terrorism and disaster-related information reaches government decision-makers. (US Department of Homeland Security, 2010, pp. 4–5)

In order to do so, OPS agents are permitted to establish user accounts on various social media sites. When appropriate (i.e. life-threatening situation), the DHS will have the ability to disclose personal social media information with foreign governments, and public and private entities. Although there is no specific mention that the DHS plans to monitor extremist behavior as detailed in this manuscript, the search terms identified in the Privacy Impact Assessment (pp. 17–21) coupled with statements made above by DHS Security Janet Napolitano, point to the real possibility of doing so in the immediate future.

Despite the popularity of mainstream social networking sites among extremist groups, some have developed their own social networking sites, including *New Saxon* by the NSM and *Stormfront.org* (Simon Wiesenthal Center, 2009). With more than 6 million posts and over 133,000 members (Big Boards, 2011), *stormfront.org* is one of the most popular white supremacist forums on the Internet.<sup>6</sup> *Stormfront.org* boasts visitors from all over the world, with most originating from the US. *Stormfront.org* forum topics include ideology and philosophy, strategy and tactics, activism (including eActivism), and legal issues, as well as, health and fitness, homemaking, education, entertainment, and financial forums.<sup>7</sup> Whereas typically hate sites function as one-way transfers of information, *stormfront.org* members can post messages, read responses, and eventually post feedback to those responses (Kim, 2005). Thus, in addition to recruitment, hate-motivated forums effectively build communities of like-minded individuals (Chau & Xu, 2006; Glaser, Dixit, & Green, 2002).

In a further attempt to build a community of like-minded individuals, white supremacists often write and speak in code, utilizing various acronyms and symbols to represent movement ideology and declarations (Simi & Futrell, 2006b). The following are examples of common acronyms and number symbols (Anti-Defamation League, 2007b). RAHOWA is an acronym for 'racial holy war' and signifies the much anticipated battle between the white race and minorities and Jews. The outcome of which will return power to the white race and Aryan rule over the world. ZOG/JOG is an acronym for 'Zionist-occupied government/Jewish-occupied government' and refers to the belief that Jews occupy, control, and dominant the government and media. WPWW is an acronym for 'White Pride World Wide' and is used primarily as a greeting among white supremacists. SWP is an acronym for 'supreme white power' and serves as the ideological basis of the white power movement. Finally, KIGY is an acronym for 'Klansman, I greet you' and is used primarily as a greeting (i.e. indicating membership and/or affiliation) among Ku Klux Klan members.



Number symbols are also used extensively among white supremacist members. For example, the number 18 represents 'Adolf Hitler'. This is accomplished by assigning numerical values to each letter of the alphabet. The first letter of the alphabet is A, whereas the eighth letter of the alphabet is H, thus AH signifies 'Adolf Hitler'. Utilizing the same method, 88 represents 'Heil Hitler' and 311 represents the KKK. Another common number symbol is 4/19, which signifies the anniversary dates of the Oklahoma City bombing (9 April 1995) and the deadly confrontation between federal agents and Branch Davidians in Waco, TX on 19 April 1993. Finally, the number 14 (words) represents the battle cry for the white power movement, that is 'We must secure the existence of our people and future for white children' and the number 5 (words) represents a code of silence used to avoid legal prosecution, that is 'I have nothing to say'.

Drawing from both face-to-face and telephone interviews with white power activists across more than 20 states, Simi and Futrell (2006b) found that 65% agreed or strongly agreed that the Internet was vital to white power activism. More specifically, activists argued that the Internet increased communication between those spatially disconnected, provided moral support, and played a vital role in planning 'real-world' events. Nevertheless, cyber-presence alone will not sustain the white power movement. In other words, a strong web-presence must be linked to real-world contexts. Examples include the White Heritage Christian Festival (affiliated with the Ku Klux Klan), hate rock music festivals, and/or Keystone State Skinhead<sup>8</sup> picnics.

According to Simi and Futrell (2006a), white supremacist groups see children as essential to the vitality of the movement. Many homes display Aryan-themed posters, wall hangings, books, and flags. Racist clothing, jewelry, and hats are commonly worn in and around the home. Finally, racist and anti-Semitic rituals are created and assimilated into everyday family life (e.g. Klan and swastika themed birthday cakes are common).

Building upon these teachings in the home, white supremacist groups have implemented various Internet recruitment strategies in an effort to attract children and teenagers. Methods include the use of brightly colored websites with balloon lettering, cartoons, coloring books, and crossword puzzles (Lamberg, 2001). Some groups even provide various links intended to assist children and teenagers with homework. For example, the *Knights Party Youth Corp of the Ku Klux Klan*<sup>9</sup> provides some of the following links: 'Youth News', 'What is the KKK?', 'Doing a school report about the KKK', 'Are there women and kids in the KKK,' 'But, I know some really nice black people', and 'Black history Myths'. This is disturbing, given that more than half of those aged between 9 and 17 years use the Internet as their primary source for homework help. Lamberg (2001) further argues that those adolescents who feel isolated and/or persecuted by classmates may be more easily swayed and/or feel empowered by joining such groups.

Other methods of attracting and recruiting children and adolescents to the white power movement include joke pages and interactive video games (Selepak, 2010). These games look and operate similar to more mainstream games but typically involve shooting and killing homosexuals, blacks, and other minorities. Titles include 'Watch Out Behind You Hunter – Shoot the fags before they rape you!', 'Border Patrol – Don't let those spics cross our border!', and 'Kaboom – the suicide bombing game'.

With more than 300 bands spanning 22 countries, white power music or 'hate rock' is becomingly an increasingly popular adolescent recruitment tool. Representing one of the most pervasive forms of racist expression, hate rock consists of violent, hateful, and profane lyrics set to heavy metal music (Schafer, 2002). The nature of the music itself (i.e. loud and rebellious) often appeals to adolescents who would not ordinarily listen to such music. Generally, it is hoped that the adolescent will eventually become desensitized to the racist messages and eventually accept extremist organizational beliefs. This was exactly the mission of Panzerfaust records (now Free Your Mind Productions<sup>10</sup>), who during a 2004 campaign attempted to distribute 100,000 hate-music CD samplers across the country to unsuspecting youths aged 13–19. The CDs were handed out in schools, university campuses, shopping malls, and parties. Dubbed 'Project Schoolyard USA', Panzerfaust solicited help from the white power community asking them to buy and distribute sampler CDs at only 15 cents apiece. Although difficult to gage the success of the campaign, Panzerfaust states the following on their website.<sup>11</sup>

Unfortunately, all good things must come to an end. Project Schoolyard USA was a huge success and it reached thousands of White Youths all across the world with the message of White survival. Everyone that was involved with Project Schoolyard would like to sincerely thank everyone who helped to make it a success. Although our main effort has come to an end, it's still possible to make your own CDs for distribution. Stay tuned in the coming weeks for instructions, graphics, etc. that you can use to spread the word.

Moreover, Futrell, Simi, and Gottschalk (2006, p. 282) argue that 'The Internet is critical to organizing the WPM [White Power Movement] music scene'. Popular US labels such as *Resistance Records* and *Free Your Mind Productions* have harnessed the power of the Internet in many ways.<sup>12</sup> These labels offer free MP3s, 24-h streaming radio and videos, chat rooms, and information concerning concerts (e.g. hotels, restaurants, and carpools available to concert goers). Other services include real-time access to live music events, photos, and sound clips, essentially allowing those to virtually attend concerts.

### **Publicity**

Extremist websites employ three rhetorical structures when justifying their reliance on violence to affect political, social, or religious change (Weimann, 2004). First, extremist websites portray their members as underdogs, with no choice but to use violence. Extremist organizations are persecuted by a relentless and oppressive enemy with violence seen as the only response. Extremist groups are portrayed as small, weak, and hunted, while governments are characterized as murderers seeking slaughter and genocide. Second, extremist organizations actively attempt to demonize and dehumanize the enemy. Members are presented as freedom fighters against a ruthless and crushing enemy. Using selected facts, misleading statements, and smear campaigns, extremist organizations effectively shift responsibility of violence from them towards their enemies (Cohen, 2002). In addition, extremist websites are increasingly using nonviolent communication in an attempt to contradict their violent image. This tactic is especially apparent with white supremacist sites, actively

promoting social creativity and social conflict rather than violence (Douglas, McGarty, Blum, & Lala, 2005).

Nevertheless, in order to attract public attention, extremist groups must have the ability to publicize their causes and activities. In the past, the act of securing the attention of the public required and often depended on attracting the attention of traditional television, radio, and print media (Furnell & Warren, 1999). Today, the Internet has given extremist groups unprecedented control over their message, providing them the ability to directly shape public perception. Chat rooms, websites, and bulletin boards are largely free from government control and censorship, essentially becoming an extremist's private television or radio network (Thomas, 2003). In fact, the Ku Klux Klan broadcasts a weekly television news show over the Internet, known as 'This is the Klan'.<sup>13</sup>

### ***Risk mitigation***

Today, extremist groups are unstructured with most members operating independently of each other. They are less command driven, and principles, rather than hierarchy, guide decisions and behavior (Arquilla & Ronfeldt, 1996). Many utilize a strategy known as leaderless resistance, which 'entails a general endorsement of terrorist violence by movement leaders but leaves planning and executing operations to individuals and small groups' (Council on Foreign Relations, 2004, para. 15). Popular among hate extremists and right wing groups, this strategy encourages individuals to commit autonomous attacks in an uncoordinated but united campaign (FBI, 2001). Facilitated by information and communication technologies, decentralized groups are inherently flexible, able to adapt quickly to changing situations and are able to capitalize on the talents of all its members (Zanini & Edwards, 2001). In fact, the white power movement is becoming increasingly international, as supremacists see themselves as part of a global movement (Simi & Futrell, 2006a). One such method includes the use of language translation engines. These powerful Internet tools essentially allow one to view the content of any website in a variety of different languages, by simply clicking a button. See the Aryan Nations website for an example of this technology in use.<sup>14</sup> Other examples of such technology include encrypted email, anonymous email accounts, and chat rooms. In addition, extremists hide text in spam, create short-term America Online Instant Messenger (AIM) accounts, and make widespread use of speech compression technology (Thomas, 2003). Needless to say, advances in information and communication technologies coupled with changes in group organizational structure has inhibited our understanding of extremist networks.

### **Conclusion**

As indicated throughout this manuscript, hate groups are exploiting Internet technologies at an increasingly alarming rate. This growth in popularity can be attributed to many factors, including easy access, fast and anonymous communication with like-minded individuals, inexpensive development and maintenance of a web presence, and a true multimedia environment. Information placed on the Internet by extremist groups include history and organizational activities, biographies of leaders, founders, and heroes, up-to-date news, training manuals, and fundraising activities. With most, if not all such groups using the Internet to spread messages of hate and violence, the

following paper examined Internet facilitation of information sharing, fundraising, social networking and recruitment, publicity, and risk mitigation.

Prior to the advent of the Internet, hate groups spread their messages of hate through the distribution of printed books, newspapers, magazines, and newsletters. Reaching only a limited number of people, these methods proved costly and largely ineffective. Today, users can instantly download (and disseminate) fliers, books, magazines and newsletters, as well as, watch and listen to recorded or live streaming audio and video in the privacy of their own homes. Other information widely available, include numerous tutorials on building bombs, firing weapons, physical fitness training, plotting assassinations, wilderness survival training, and how to organize and manage an extremist cell.

Similar to tactics used to share ideological and other information, the Internet has also proven to be an effective social networking tool. One method extremely popular among white supremacists entails the creation of electronic bulletin boards or forums designed explicitly for their target audience. Whereas websites function as one-way transfers of information, forums allow members to post messages, read responses, and eventually post feedback to those responses; effectively building communities of like-minded individuals.

In addition to social networking, white supremacist groups have found the Internet to be a powerful recruitment tool. Seeing children as essential to the vitality of the movement, hate groups have implemented various recruitment strategies in an effort to attract children and teenagers. Methods include everything from 'child-friendly' websites and video games, to the ever-growing popularity of hate rock music.

Additionally, this paper addressed how Internet technologies have given white supremacist groups unfettered control over their message, providing them the ability to directly shape public perception. In other words, these groups no longer must solely depend on the traditional media to publicize their causes and activities. Finally, this paper addressed the value of the Internet in terms of risk mitigation.

In closing, it is worth revisiting a 2009 report prepared by the Extremism and Radicalization Branch, Homeland Environment Threat Analysis Division. This report suggests that the rightwing extremist Internet chatter indicates that: 'The economic downturn and the election of the first African American president present unique drivers for rightwing radicalization and recruitment' (p. 2). The report further argues that the three officers killed in Pittsburgh, Pennsylvania, on 4 April 2009, by a racist gunman, and the planned but disrupted attack on then senator Barack Obama in the run-up to the 2008 presidential election, point to an escalation in rightwing extremist violence.

Moreover, according to a recent White House Terrorism Strategy (2011):

The United States Constitution recognizes freedom of expression, even for individuals who espouse unpopular or even hateful views. But when individuals or groups choose to further their grievances or ideologies through violence, by engaging in violence themselves or by recruiting and encouraging others to do so, it becomes the collective responsibility of the US Government and the American people to take a stand. (p. 1)

The above quote seems to address the complex problems that arise when balancing societal concerns against constitutional guarantees of free expression. In fact, pushing a community-based educational approach, White House officials plan to educate and assist community members and law enforcement professionals about

the dangers of online extremism. Hence, future research should continue to examine and understand Internet usage by these groups.

## Notes

1. <http://www.stormfront.org>.
2. <http://www.skrewdriver.net/zogopp1.html>.
3. <http://www.skrewdriver.net/fmintro.html>.
4. See, e.g. <http://www.kelticklankirk.com>.
5. See, e.g. <http://www.aryanwear.com>.
6. More than just simply visiting or browsing the site, membership requires users to provide limited personal information and register a username and password, similar to more mainstream social networking sites.
7. <http://www.stormfront.org>.
8. <http://www.kss88.com/>.
9. <http://www.kkk.bz/youthcorp.htm>.
10. <http://www.freeyourmindproductions.com/>.
11. <http://www.freeyourmindproductions.com/sampler/>.
12. <http://www.resistance.com/>.
13. <http://www.whitepride.tv/>.
14. <http://www.aryan-nations.org/index-2.htm>.

## Notes on contributor

W. Chris Hale is an Assistant Professor of Criminal Justice at Louisiana State University in Shreveport. He has published and presented research in the areas of cybercrime, terrorism, and intelligence analysis. Most recently, he has published a co-authored book entitled *Wicked Shreveport* and has had work published in the *Proteus futures digest* and the *International Journal of Emergency Management*, among others.

## References

- Adams, J., & Roscigno, V.J. (2005). White supremacists, oppositional culture and the World Wide Web. *Social Forces*, 84(2), 759–778.
- Anti-Defamation League. (2007a). *Racist skinhead project*. Retrieved November 22, 2007, from the Anti-Defamation League website: [http://www.adl.org/racist\\_skinheads/](http://www.adl.org/racist_skinheads/)
- Anti-Defamation League. (2007b). *Hate on display: a visual database of extremist symbols, logos, and tattoos*. Retrieved November 22, 2007, from the Anti-Defamation League website: [http://www.adl.org/hate\\_symbols/default.asp](http://www.adl.org/hate_symbols/default.asp)
- Ariza, L. (2006). Virtual jihad. *Scientific American*, 294(1), 18–21.
- Arquilla, J., & Ronfeldt, D. (1996). *The advent of netwar* (MR-789-OSD). Santa Monica, CA: Rand.
- Associated Press. (2010, June 18). Napolitano: Internet monitoring needed to fight home-grown terrorism. *Associated Press*. Retrieved October 21, 2011, from <http://www.ap.org>
- Berger, J. (2009, June 11). Holocaust museum shooting shows difficulties in tracking hate sites, speech. *Fox News.com*. Retrieved October 21, 2011, from <http://foxnews.com>
- Big Boards. (2011). *Statistics for stormfront*. Retrieved October 21, 2011, from the Big Boards website: <http://rankings.big-boards.com/?p=all>
- Bostdorff, D.M. (2004). The internet rhetoric of the ku klux klan: A case study in web site community building run amok. *Communication Studies*, 55(2), 340–361.
- Bullard, S. (1991). *The ku klux klan: A history of violence and racism*. Montgomery, AL: Southern Poverty Law Center.
- Chau, M., & Xu, J. (2006). *A framework for locating and analyzing hate groups in blogs*. Paper published in the Proceedings of Pacific-Asia Conference on Information Systems, Kuala Lumpur, Malaysia, 6–9 July 2006.
- Cho, J.H., & Tomkins, A. (2007). Social media and search. *IEEE Internet Computing*, 11, 13–15.



- Cohen, F. (2002). Managing network security: Terrorism and cyberspace. *Network Security*. Retrieved November 27, 2006, from the Network Security website: <http://all.net/journal/netsec/2002-05.html>
- Conway. (2005). *Terrorist use of the Internet and fighting back*. Paper presented at the Cybersafety: Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities, Oxford Internet Institute (OII), Oxford University, UK, 8–10 September 2005.
- Council on Foreign Relations. (2004). *American militant extremists: United States, radicals*. Retrieved June 8, 2005, from <http://www.cfrterrorism.org>
- Dees, M. (1996). *Gathering storm: America's militia threat*. New York, NY: Harper Perennial.
- Dodds, P. (2011, September 29). Extremist groups grow through Facebook and other social media. *MercuryNews.com*. Retrieved October 21, 2011, from <http://www.mercurynews.com>
- Douglas, K.M., McGarty, C., Blüch, A., & Lala, G. (2005). Understanding cyberhate: Social competition and social creativity in online white supremacist groups. *Social Science Computer Review*, 23(1), 68–76.
- Espiner, T. (2009, March 18). UK to monitor, store all social-network traffic? *CNET News*. Retrieved October 19, 2011, from <http://www.news.cnet.com>
- Extremism and Radicalization Branch, Homeland Environment Threat Analysis Division. (2009). *Rightwing extremism: Current economic and political climate fueling resurgence in radicalization and recruitment* (IA-0257–09). Washington, DC: DHS/Office of Intelligence and Analysis.
- Facebook. (2011). *Facebook statistics*. Retrieved October 21, 2011, from the Facebook website: <http://www.facebook.com>
- Feagin, J., & Vera, H. (1995). *White racism*. New York, NY: Routledge.
- Federal Bureau of Investigation. (2001). *Terrorism 2000/2001*. Retrieved June 8, 2005, from [http://www.fbi.gov/publications/terror/terror2000\\_2001.htm](http://www.fbi.gov/publications/terror/terror2000_2001.htm)
- Federal Bureau of Investigation. (2008, July 7). *White supremacist recruitment of military personnel since 9/11* (Intelligence Assessment). FBI Counterterrorism Division.
- Federal Bureau of Investigation. (2010, September 22). Robert S. Mueller, III, Director, Federal Bureau of Investigation, Statement before the Senate Committee on Homeland Security and Governmental Affairs, Washington DC. (Testimony). Retrieved October 17, 2011, from <http://www.fbi.gov>
- Furnell, S., & Warren, M. (1999). Computer hacking and cyber terrorism: The real threats in the new millennium. *Computers and Security*, 18(1), 28–34.
- Futrell, R., Simi, P., & Gottschalk, S. (2006). Understanding music in movements: The white power music scene. *The Sociological Quarterly*, 47, 275–304.
- Glaser, J., Dixit, J., & Green, D.P. (2002). Studying hate crime with the internet: What makes racists advocate racial violence? *Journal of Social Issues*, 58(1), 177–193.
- Jenkins, P. (2003). *Images of terror: What we can and can't know about terrorism*. Edison, NJ: Aldine Transaction.
- Kaplan, E. (2006). *Terrorist and the Internet*. Retrieved November 6, 2006, from <http://www.cfr.org/publications/10005/>
- Kim, T.K. (2005). *Electronic storm: Stormfront grows a thriving neo-Nazi community*. Retrieved November 11, 2007, from the Southern Poverty Law Center website: <http://www.splcenter.org/intel/intelreport/article.jsp?aid=551>
- Kleg, M. (1993). *Hate prejudice and racism*. Albany, NY: SUNY Press.
- Lamberg, L. (2001). Hate-group web sites target children, teens. *Psychiatric News*, 36(3), 26.
- MacDonald, A. (1978). *The turner diaries*. Washington, DC: National Vanguard Press.
- MacDonald, A. (1989). *Hunter*. Washington, DC: National Vanguard Press.
- Martin, G. (2011). *Terrorism and homeland security*. Thousand Oaks, CA: Sage.
- Paul, I. (2011, September 13). Americans are drawn to social networks, with Facebook leading the way. *PCWorld*. Retrieved October 21, 2011, from <http://www.pcworld.com>
- Perry, B. (2000). 'Button-down terror': The metamorphosis of the hate movement. *Sociological Focus*, 33(2), 113–131.
- Plushnick-Masti, R., & Nephin, D. (2009, April 4). Richard Poplawski, Pittsburgh gunman, kills 3 police officers. *The Huffington Post*. Retrieved October 21, 2011, from <http://www.huffingtonpost.com>



- Rainie, L., Purcell, K., Goulet, L.S., & Hampton, K.N. (2011, June 16). Social networking sites and our lives. *Pew Research Center Publications*. Retrieved October 24, 2011, from the Pew Research Center website: <http://www.pewresearch.org>
- Ridgeway, J. (1995). *Blood in the face*. New York, NY: Thunders Mouth Press.
- Schafer, J.A. (2002). Spinning the web of hate: Web-based hate propagation by extremist organizations. *Journal of Criminal Justice and Popular Culture*, 9(2), 69–88.
- Selepak, A. (2010). Skinhead super Mario brothers: An examination of racist and violent games on white supremacist web sites. *Journal of Criminal Justice & Popular Culture*, 17(1), 1–47.
- Simi, P. (2010). Why study white supremacist terror? A research note *Deviant Behavior*, 31, 251–273.
- Simi, P., & Futrell, R. (2006). White power cyberculture: Building a movement. *The Public Eye Magazine*, 20(2), 1, 7–12.
- Simi, P., & Futrell, R. (2006). Cyberculture and the endurance of white power activism. *Journal of Political and Military Sociology*, 34(1), 115–142.
- Simon Wiesenthal Center. (2009). *Facebook, YouTube+: How social media outlets impact digital terrorism and hate* (Museum of Tolerance New York). Retrieved October 24, 2011, from the Simon Wiesenthal Center website: <http://www.wiesenthal.com>
- Simon Wiesenthal Center. (2011). *2011 Digital terrorism & hate report*. Retrieved October 17, 2011, from the Simon Wiesenthal Center website: <http://www.wiesenthal.com>
- Southern Poverty Law Center (SPLC). (2011). *Active US hate groups in 2010*. Retrieved October 21, 2011, from the Southern Poverty Law Center website: <http://www.splcenter.org/get-informed/hate-map>
- Stern, K.S. (1999). *Hate and the Internet*. New York, NY: American Jewish Committee.
- Thomas, T.L. (2003). Al Qaeda and the Internet: The danger of ‘cyberplanning’ [Electronic version]. *Parameters*, 33(1), 112–123.
- US Department of Homeland Security. (2010). *Privacy impact assessment for the office of operations coordination and planning publicly available social media monitoring and situational awareness initiative*. Washington, DC: US Department of Homeland Security.
- Weimann, G. (2004). *www.terror.net: How modern terrorism uses the Internet*. United States Institute of Peace, Special, Report, 116.
- Weimann, G. (2006). *Terror on the Internet: The new arena, the new challenges*. Washington, DC: United States Institute of Peace Press.
- White House Terrorism Strategy. (2011). *Empowering local partners to prevent violent extremism in the United States*. Washington, DC: The White House.
- Yang, M., Kiang, M., Ku, Y., Chiu, C., & Li, Y. (2011). Social media analytics for radical opinion mining in hate group web forums [Electronic version]. *Journal of Homeland Security and Emergency Management*, 8(1), 1–17.
- Zanini, M., & Edwards, J.A. (2001). The networking of terror in the information age. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 29–60). Santa Monica, CA: Rand.
- Zhou, Y., Qin, J., Lai, G., Reid, E., & Chen, H. (2006). Exploring the dark side of the web: Collection and analysis of US extremist online forums. In S. Mehrotra, D.D. Zeng, H. Chen, B. Thuraishingham, & F. Wang (Eds.), *ISI 2006, LNCS 3975* (pp. 621–626). Berlin: Springer Verlag.