

Dark Hatred: Antisemitism on the Dark Web

Lev Topor

Abstract

Antisemitism is racism. While it is not broadly accepted in modern societies, it does exist in the margins, in places with no norms or regulations. The key purpose of this article is to develop a new conceptual research framework for the study of both antisemitism and racism. The dark web hosts a great deal of offensive and criminal activity; it also hosts racist and antisemitic activity. It is necessary, then, to search the dark web, the dank underbelly of society, for activity which is not accepted in conventional life. In order to make this conceptual research framework available to other researchers, an overview of racist antisemitic activity on the dark web will be presented and analyzed. As concluded, governments do not take sufficient action for the eradication of dark web racism as it is hidden from society and is very difficult to regulate. In contrast to the surface web, racists, antisemites, thrive there.

Keywords: Antisemitism, Racism, Dark Web, Deep Web

INTRODUCTION

Antisemitism is racism. Even if it is not widely and publicly accepted in modern liberal societies, it exists in the margins.¹ Antisemitism is present in the far left's and postcolonial left's assertions that the state of Israel has committed crimes;² it is present in the alt-right, with its neo-Nazi groups that use classic antisemitic motifs and worship Hitler's memory;³ it is present within fundamentalist Islam, which accuses both Israel and Jews in general of harming and conspiring against Muslims.⁴ Contemporary liberal society does not accept racist behavior: It stands firm against extremism and tries to cast it out.⁵ However, such ideas, and their associated activity, do not disappear. A simple ban cannot banish racism. Instead, it moves to the edges of society.

In the digital world, antisemitism finds plenty of crevices in which to hide.⁶ The key purpose of this article is to develop a new conceptual framework for the study of antisemitism

and racism. If antisemitism will not simply vanish, it is necessary to search the margins of modern society, trace it, analyze it, and eventually combat and abolish it. This article aims to present researchers with new concepts and methods to study racist and antisemitic phenomena in the digital safehouses of bigots. Unregulated places such as the deep web and dark web host a lot of offensive and criminal activity.⁷ Antisemites can express their racist ideas with almost complete anonymity and security, and with no shame at all. They do not need to fear "persecution" for their beliefs. In fact, the real problem with antisemitism and racism on the dark web is its normality. Such online racism is likely to incite hatred in society and serve as a "call to action" against those presented as harmful by the racists.⁸

This article aims to present and discuss research on antisemitism, and racism per se, in a largely invisible area of society—the dark web. Methodologically, a conceptual analysis

of antisemitism combined with empirical evidence from the dark web is utilized.⁹ Firstly, I will present a nontechnical explanation of the deep web and dark web, in order to provide researchers with ways to approach these entities. Secondly, I will present the conceptual and methodological framework, with the aim of explaining the reasons for this exploration into “hidden worlds.” Thirdly, I will analyze antisemitic activity on the deep web and dark web, describing contemporary, anonymous, and shameless racist and antisemitic behavior. For comparison, I will examine antisemitic activity on the “surface web”—that is, the web most commonly used in day-to-day life. I will conclude by sketching an image of the future of research on racism and antisemitism and the role of the deep web and dark web in such research.

THE DEEP WEB AND DARK WEB: WHAT ARE THEY, HOW TO ACCESS THEM, AND WHAT TO LOOK FOR?

What They Are

The deep web is everything that is not on the controlled and indexed surface web. The surface internet began as the Arpanet, a project of the United States Department of Defense. In 1983, the Arpanet switched from being a closed network, named the Network Control Protocol (NCP), and became an open one—the Transmission Control Protocol/Internet Protocol (TCP/IP). Moving from a closed circuit to an open one led to the expansion of these protocols and communication types. As the number of networks and users grew, a classification of networks began: National (Class A), Regional (Class B), and Local (Class C). Today, every government and individual can design and install his own network.¹⁰

Accelerating the internet’s development and expansion, the Internet Corporation for Assigned Names and Numbers (ICANN) started designing the internet to be more accessible to the public. It turned into something

very like the *Yellow Pages*. ICANN gave names—IPs, and Domain Name Systems (DNS)—to computers in every government, industry, home, and eventually our mobile and smart devices.¹¹ Now, ICANN’s websites can be found easily. Instead of typing an IP address (e.g., 192.0.32.7), people can simply type “icann.org.”¹²

Thus, ICANN began indexing every registered service, invited big tech giants (such as Google, Bing, Yahoo, AOL, Yandex.ru, and others) to index, sort, and manipulate/adapt all of the registered DNSs and IPs.¹³ That indexing process raises some questions and concerns. First, who gets to be at the top of the index list, and why? Manipulation the indexing process can be exploited by governments, companies, and so forth. Second, if every address is indexed, it can be monitored by the government, commercial players, and even malicious players. In short, this is a danger to free speech (racist speech).¹⁴ Denying someone access to the internet is a violation of basic human rights.¹⁵ Moreover, oppressive countries use IP addresses to silence opposition simply by tracing them and arresting the owners.¹⁶

Moreover, in Foucauldian terms, the hegemony of US-based Arpanet, internet, and indexing systems can lead to the exclusion of weaker, un-indexed, players; hence the popularity of the dark web.¹⁷ While the internet is now global and can seem free and equal, it is not. The ones who control the internet, such as the United States or companies such as Google, promote their preferred sites, ideologies and information. When certain information is promoted other information is left behind. Countries can restrict their internet networks as well. Such is the Chinese case: China restricts anti-Chinese sites in order to prevent its citizens from reaching it.¹⁸

The deep web is everything that is not indexed by search engines and regulators: dynamic web pages that are generated by requests; blocked sites that use authentication methods; unlinked sites which prevent an effective

indexing process; non-scriptural or contextual content (everything that is not based on HTML); limited-access networks which are placed in non-public infrastructures; and private web platforms which require a password or a payment for access.¹⁹

As mentioned above, it is important to note the role of search engines when comparing the deep web and the surface web. Currently, search engines systematically exclude, either by design or by accident, certain sites in favor of others. Nations and giant tech companies manipulate and control the web when they refuse to index a site or when they rank a certain site lower than other sites so the lower ranked site is harder to find. In this way, free speech is prevented. Certain groups of people, legitimate or not, turn to the deep web and the dark web to avoid this kind of political or corporate interference.²⁰

Lastly, dark webs and other alternative routing infrastructures are hosted on platforms which require special and specific software to reach them, such as the most commonly used dark web, TOR²¹ browser.²² Other examples for popular dark webs are I2P, Riffle, and Freenet. In essence, if I (the author of this paper) set up a private server in my house, for which special software is also required (such as a special browser) and give you (the reader) the address and the password, we would be on our own dark web.

How to Access Them

The deep web can be accessed in a variety of ways. In order to understand how to explore it, a distinction must be made between the deep web and the dark web. The dark web is part of the deep web but can only be accessed with special software because it is based on a unique infrastructure. TOR, I2P, Freenet, and Riffle are such infrastructures. The deep web is everything that is not indexed: Some of it can be accessed through regular browsers, but one must know the address and the content first.²³ If regulators do not know where to look, evil activity can flourish there: terrorist plots, hacking and

extortion, pedophile ring, drugs and arms distribution, human trafficking, cyberattacks, and, of course, extreme and malicious manifestations such as fundamentalist Islam and neo-Nazism. The dark web is a double-edged sword: It enables free speech, but spreads extremism.²⁴

An example of unique deep web infrastructure is TOR—probably the best-known access tool. The TOR network originated in the US Naval Research Laboratory and was introduced in 2002, with the aim of facilitating secure military and governmental communication worldwide.²⁵ TOR allows anonymous communication between users, clients, and servers by using volunteer nodes (crossroads). All routing is encrypted and, while some nodes can be exposed, it is almost impossible to retrieve *all* of the access points and nodes from server to client. Thus, if one were to enter a special address, the last node accessing the address could be found but not the original user. Search engines and governments can do very little to sort the dark web. The TOR network uses unique .onion domain names that are not accessible by regular surface web browsers.²⁶

While network analysis can detect these kinds of connections, it cannot reach the content. Dark web users could be discovered by a simple deprivation methodology—every transaction of data that local ISPs can see is innocent and everything the ISPs cannot see, or reach, is an abnormal activity such as governmental opposition or intelligence agents. As the US initiated and used the dark web for its intelligence proposes, it had no choice but to flood the world with dark web users in order to make the deprivation methodology harder for utilization. It promoted the dark web, specifically TOR project, as a good mechanism for regime opposition in oppressive regimes and for the promotion of human rights.²⁷ By contrast, unintentionally, the US is responsible for some of the illegal, racist, and terrorist activity on the dark web since it provides the anonymity platform for all, those who use it for good and those who abuse it.²⁸

What to Look For

The deep web and dark web's privacy and security enable a vast amount of illegal and harmful activity. If volunteer, or exploited nodes, cannot help society regulate and track harmful activity, then one of the ways to do so is by creating and distributing regulated nodes. Typically, government-made nodes will track every motion, allowing the government to trace the route back to the real user. Another way to track harmful activity is to constantly monitor hidden services and hidden social networks, try to map them, and index information semi-manually in order to note overlapping information.²⁹ As most illegal activists change their domains and designs constantly, this latter approach is often unhelpful.

DARPA's (Defense Advanced Research Projects Agency) Artificial Intelligence (AI) MEMEX software is another tool with which security agencies monitor dark webs. Instead of using the kind of preprogrammed and pre-designed software most of the search engines employ, MEMEX uses AI to explore and catalogue the dark web.³⁰ Another sociological method is time-zone geolocation of crowds who use the dark web. This method allows for the analysis and comparison of populations in dark web in certain locations to the regulated activity of surface web populations.³¹

A social researcher that wants to analyze and gather information on the dark web must take several precautions before entering and exploring it.³² Considering the fact that the deep web contains ninety to ninety-five percent of web content, it is nearly impossible to explore it with any thoroughness.³³

Research on the dark web can be regarded as a sociological and ethnographical research. Social researchers can take interest in blogs, forums, boards, marketplaces, and even social networks similar to Facebook: They host a fascinating variety of activity and opinion in an unmonitored, anonymous way.³⁴ An individual can express their views candidly, without self-censorship: They do not have to worry about the way society

will perceive them. Several research methods can be applied to analyze social, specifically antisemitic, activity on the dark web: surveys, experiments, case studies, interpretive research, and interviews.³⁵

Entering the Hidden Wiki, a directory of hidden links to hidden services and places, several things can be found: search engines, financial services, commercial services and marketplaces; domain and web hosting services, hacking services, pornography, drugs, arms, pirate audio and video exchanges, and much more. The important platforms the present study on racism and antisemitism are blogs, forums, boards, and social networks.³⁶ In addition, popular search engines are used to search for dark web sites and content. Typing the word "Jews" or "Israel" in popular search engines, such as Ahmia.fi³⁷ or Torch,³⁸ brings up very disturbing antisemitic content.

CONCEPTUAL FRAMEWORK

In August 2017, Heather Heyer, 32, was killed when a white supremacist drove a car into a demonstration against an alt-right rally—called "Unite the Right"—in Charlottesville, Virginia.³⁹ One of the organizing bodies of that alt-right rally was the neo-Nazi site the *Daily Stormer*.⁴⁰ This incident led to an unofficial ban on the site. Companies such as Google, GoDaddy, and other internet and technology providers refused to give this neo-Nazi site access their platforms. The *Daily Stormer* was driven off the surface web. However, it quickly found a new home, somewhere beyond the reach of social norms of behavior and with almost no regulations⁴¹—the deep web and the dark web. With its last gasp, and with help from supporters and followers, the *Daily Stormer* published a link to its new .onion address.⁴²

One can argue that society, specifically private tech giants, played a crucial role in the eradication of racism and antisemitism after Charlottesville. A significant number of far-right sources which disseminated socially

unacceptable antisemitic and racist views vanished from the surface web.⁴³ But the reality is much more complicated. The Charlottesville rally and the banning of the *Daily Stormer* is a particularly valuable case for research. Antisemitism is difficult to regulate on the internet: Laws on racism and incitement effectively only emerged in the last decade. Furthermore, there is a geographical jurisdiction difficulty with web antisemitism and extremism in general. If an antisemitic statement or incitement is made in a country where it is legal, can a country in which antisemitism is illegal take action against the racists involved? A digital post can spread across the whole world. What is a tech company's position with regard to national and international law?⁴⁴

The *Daily Stormer* case is of special interest. It was one of the most successful racist sites online, alongside veteran sites like *Stormfront*⁴⁵ and *Jew Watch*.⁴⁶ These sites had also been banned, taken offline, or sanctioned in the past.⁴⁷ However, unlike the *Daily Stormer*, *Stormfront* and *Jew Watch* are still online with their original domains. The *Daily Stormer*'s problem was that it transposed web racism and incitement to the real world. What happened in Charlottesville was violent extremism and terrorism, which eventually took a life. Thus, a difficult question must be asked: What was the real reason for the tech giants to act against the *Daily Stormer*? Was it because of normative criticism (most importantly, media pressure) and mainstream opposition to racism and antisemitism, or was it the horrible manner of Heather Heyer's death and homeland security concerns?

As argued by Andre Oboler of the Online Hate Prevention Institute, governments have recently increased their efforts to tackle hate speech, incitement, and violent extremism on the surface web.⁴⁸ Racist activity on the surface web is no longer tolerated. Social media platforms and tech companies are being directly instructed by governments to control racism and extremism online. Moreover, governments are looking to increase legislation to better

police the surface web. For instance, Germany investigated and opened a prosecution against Facebook over hate posting in late 2015. Following a public outcry and German political pressure, Facebook hired specialists to monitor and delete racist posts.⁴⁹

Though there is an increase in public and governmental understanding of web racism and antisemitism, a recent study showed this understanding drops behind the actual trends of web antisemitism. A study by the World Jewish Congress shows that there has been a dramatic increase of thirty percent in antisemitic posts and holocaust denial on the web and social media.⁵⁰ A study by the Anti-Defamation League (ADL) presents data for a worrying increase in online antisemitism.⁵¹ The Federal Bureau of Investigation (FBI) recorded 58.1 percent of religious hate crimes victims targeted Jews in 2017.⁵²

The established antisemitism of the *Daily Stormer* had not vanished away but moved to a different platform. Another *Unite the Right* rally took place in August 2018, this time in Washington, DC.⁵³ While it is true that American free speech laws allow these kinds of racist rallies and activities to take place,⁵⁴ it is also true that the participants at Charlottesville—mostly nationalists, neo-Nazis, and Ku Klux Klan members—did not have any difficulty organizing the DC hate rally, even if they were eventually outnumbered by anti-racist groups who tried to prevent the rally.⁵⁵

The *Daily Stormer* continued, without any interruptions, on its dark web site. Just before the rally took place, the dark web site was used as a bulletin board. It stated that an old *Daily Stormer* domain⁵⁶ was working on the surface web and that, if this domain was seized again, the site would return to the dark web.⁵⁷ Thus, the *Daily Stormer* helped gather racist supporters for a "Unite the Right" rally once again.⁵⁸ Right after the rally, in a cynical article from August 13, 2018 the murdered Heyer was shamelessly and hatefully mocked.⁵⁹

* * *

There are differences between the types of antisemitism which are mostly present on the dark web. These are distinguished in the way society perceives them. Currently, one type is found mostly on the new and extreme left. Left antisemitism presents itself as criticism of Israeli policies and even anti-Zionism. It argues that Israel, and its Jewish supporters, are doing harm to the Palestinians and the Middle East. As it is artists and scholars who make up a good number of these anti-Israel left activists, they are not considered a national security threat in the same way that the right-wing nationalists are. Although criticism of any conflict is welcome, the left uses antisemitic stereotypes and motifs to criticize Israel.⁶⁰ The extreme left is being “pushed” into antisemitic behavior and this fact must be emphasized. That is, actions meant to harshly criticize, which are not antisemitic, can actually have an effect of actions which are antisemitic. Thus, mainstream society accepts the far left’s views and they continue to flourish in anti-Israeli and BDS⁶¹ movements under the sign of critique. The right, however, does not hide its antisemitism in normative factors.⁶²

The second type of antisemitism is found in alt-right movements and in fundamentalist Islamist circles. In contrast to the leftist version of antisemitism, extreme Islamists and the alt-right do not try to explain or disguise their hatred and prejudice. This kind of direct and overt antisemitism presents the Jewish people as inferior to the white race or to Muslims.⁶³ It openly taints the Jewish people and the state of Israel. Unlike left antisemitism, these racist acts are not accepted by society and are shunted to its outskirts when they gain a certain amount of publicity or start having an impact on real life. However, Islamicist and alt-right antisemitism does remain active and continues to flourish in places where norms and regulations are seldom found.⁶⁴ In a recent study, Eva Kaján notes that hate speech is endorsed and promoted on the dark web. The haters unite and form a strong hate-driven ideological platform.⁶⁵

There is clearly danger. Instead of opposing, fighting, and eradicating antisemitism,

society effectively ignores it. Contemporary society believes that with a simple ban antisemitism will disappear. But it is not that easy or simple. What society actually achieves, and perhaps even wants, is merely a temporary deportation. The irony is that many antisemites begin their social media activity on the dark web. It is on the margins that their hatred grew in the first place. Putting them back there, where they have no fear of persecution, they will only become stronger. They do not need to fear a shutdown or legal action. If only society could assure that the expelled antisemites would not come back. But the issue is difficult to solve. The fear is that, if not regulated and moderated, a strain of antisemitism will erupt into the mainstream that is more powerful we have seen before.

In addition, when hidden on the dark web the scale of antisemitism is unknown. The surface web is relatively transparent and regulated: In theory, an accurate assessment of antisemitism can be made. The deep web, on the other hand, is estimated to be about 400 to 500 times larger than the surface web—and it is nearly impossible to index.⁶⁶ This compels us to ask the question: Is the dark web 400 or 500 times more antisemitic and racist than the surface web?

The simple answer is no. The deep web is indeed much larger than the surface web, but most of it is used to securely store information, such as governmental data, private and access-restricted information such as bank accounts and social network accounts. Anything that is inaccessible to the public, is password protected, and restricted counts as the deep web. The problem is present in another layer of the web: the dark web.

While antisemitic and racist activity is not 500 times greater on the dark web, it is unregulated and can be manifested more shamelessly and virulently. The dark web hosts activity that is similar to that which one sees on surface web forums, boards, marketplaces, blogs, social networks, and so forth.⁶⁷ The real issue is not one of scale: It is the lack of law-enforcement. Antisemitism on the regulated surface web can

be dealt with, removed, and blocked, thus stopping the spread of hate for a while. Antisemitism on the dark web, however, can hardly be removed and blocked.

ANTISEMITIC ACTIVITY ON THE DARK WEB

When it comes to antisemitic activity, the dark web is similar to the surface web. It has almost the same platforms. The key differences are in anonymity and regulation. While the surface web—including social media sites—can host racist and antisemitic platforms, sell antisemitic items, and facilitate antisemitic activity, some regulation and monitoring are possible and there are examples of positive action against the phenomena, as described below. By contrast, it is technically harder for authorities and technology companies to act against antisemitic activity on the dark web.

An exploration and analysis of antisemitic activity on the dark web is presented in this section with the purpose to describe contemporary anonymous and shameless antisemitic activity as well as the platforms which host it. Some of this activity is compared to cases from the surface web, where monitoring efforts are improving and the suppression of antisemitic activity takes place. The most important platforms for social scientists are presented, including sites such as market places, blogs, forums, boards, and social networks. Antisemites buy and sell antisemitic items, publish of antisemitic hate for all to read, and discuss their hatred privately with one another. Some screenshots of websites are included since .onion sites often change addresses, use generic links, and are often taken offline.⁶⁸

Marketplaces

Dark web marketplaces are filled with different illegal items. They sell pedophilic material, drugs, weapons and arms, human beings, and racist material. Nowadays, dark web marketplaces are both regulated and unregulated. This contradiction is due to the scale of these marketplaces.

They are regulated by the analysts and agents of various law enforcement agencies. Yet there is not enough law enforcement manpower available to watch these vast spaces. Since these sites are not indexed and regulated by keywords, as in the surface web, most of the marketplaces are lawless and users can buy and sell whatever they like.⁶⁹ In 2018, the US Department of Justice announced its first undercover operation targeting dark web vendors: It resulted in thirty-five arrests and the seizure of weapons, drugs, other illegal items, and more than \$23.6 million. Still, this haul represents a drop in the ocean.⁷⁰

Entering famous marketplaces such as Valhalla,⁷¹ Imperial Library⁷² or Dream Market⁷³ one is struck by the diversity of what is on offer. Apart from drugs, arms, counterfeit and stolen goods, there are banned books such as Hitler's *Mein Kampf*⁷⁴ or *The Protocols of the Elders of Zion*.⁷⁵ One can find on these marketplaces a variety of white supremacist and Nazi-related items as well. For instance, Dream Market offered Hitler gold coins (fig. 1), Nazi-themed clothes, stamps, pictures, artwork, and so forth. These marketplaces are unregulated and without limitless manpower law enforcement agencies around the world cannot hope to catch sellers. Furthermore, such sellers are not a threat to society in the same way that terrorists or hitman are.

This situation is, of course, different on the surface web where liberal society holds sway. As early as 2001, eBay banned Nazi, Ku Klux Klan, and other racist and antisemitic items. Regulation was fierce. Internet users who used French or German surface browsers were blocked from searching for Nazi-related items.⁷⁶ In 2013, following an investigation by a UK newspaper, eBay removed Holocaust objects.⁷⁷ Recently (August 2018), Amazon removed Nazi and white supremacist symbols and items from.⁷⁸ When racist and antisemitic behavior contravenes national laws, modern society acts against it, at least when large technology companies are involved. This situation also encourages tech giants to take more preemptive action themselves to ensure legal compliance.

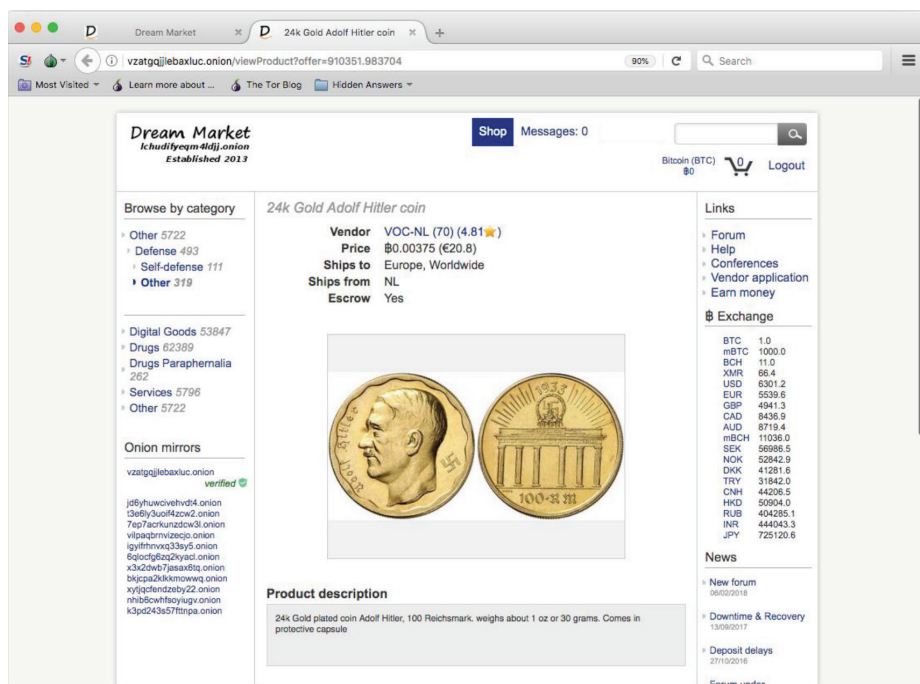


FIGURE 1. 24k gold Hitler coin for sale in *Dream Market*.

Blogs

Blogs on the dark web are another example of public racism. While finding white supremacist, Nazi, and antisemitic items on the dark webs is fairly easy, since sellers want to make a sale, blogs are a different story. A worrisome example is a blog named *White Will Survive*.⁷⁹ There, the author urges users to reproduce and distribute the stories. Posts and stories develop as references and hyperlinks to other stories. One post describes Zionists as Jews who think they have a divine right to Israel, are mentally ill, rape, and desire to kill everyone who is not Jewish. In contrast to the well-known stereotype that Jews control global finance, this blog describes them as parasites who rely on others for their money. As shown in figures 2–4, this blog is remarkably antisemitic, anti-Zionist, and over all racist.

Another example of an extreme antisemitic blog on the dark web is *Heidenwut*.⁸⁰ In a post from January 2017 the author states:

Since the Charlottesville incident we've seen a lot of pro-white websites go down. Daily stormer was even kicked off the domain name registration system and forced to retreat down into the dark net with me. Although many on the net see this as some great harbinger of doom, the fact is they should have (((shut it down))) years ago if they wanted to prevent the spread and saturation of our messages to the world.⁸¹

In another post, the author presents the idea of starting a soap company using antisemitic tropes of Jewish cuisine. Soap names include “Greedy Grape”, “Oi-Vey Orange,” and “Victim Group Vanilla.” The “Jewish Soap Idea” is illustrated in the figure below (fig. 5).

These kind of blogs and sites on the dark web are not rare. As mentioned by the *Heidenwut* blogger, the right place for them to exist is the dark web. Both dark web and surface web sites and blogs can hold similar content; the

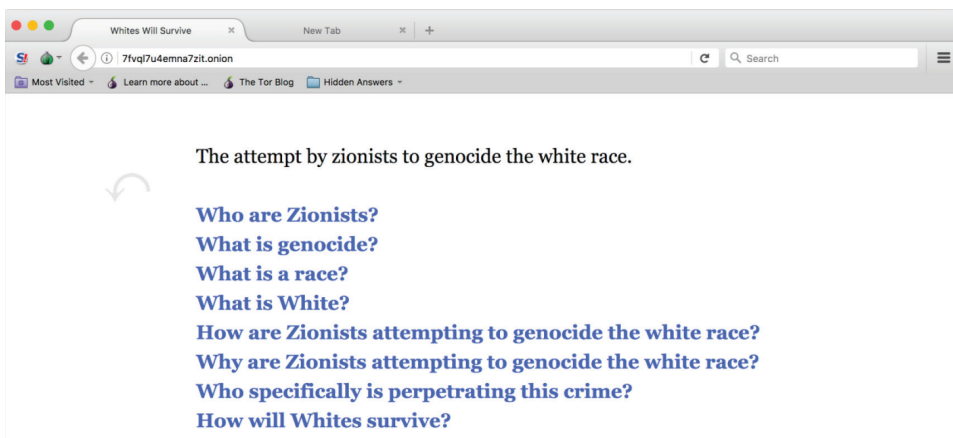


FIGURE 2. *White Will Survive* (Blog), interactive table of contents.

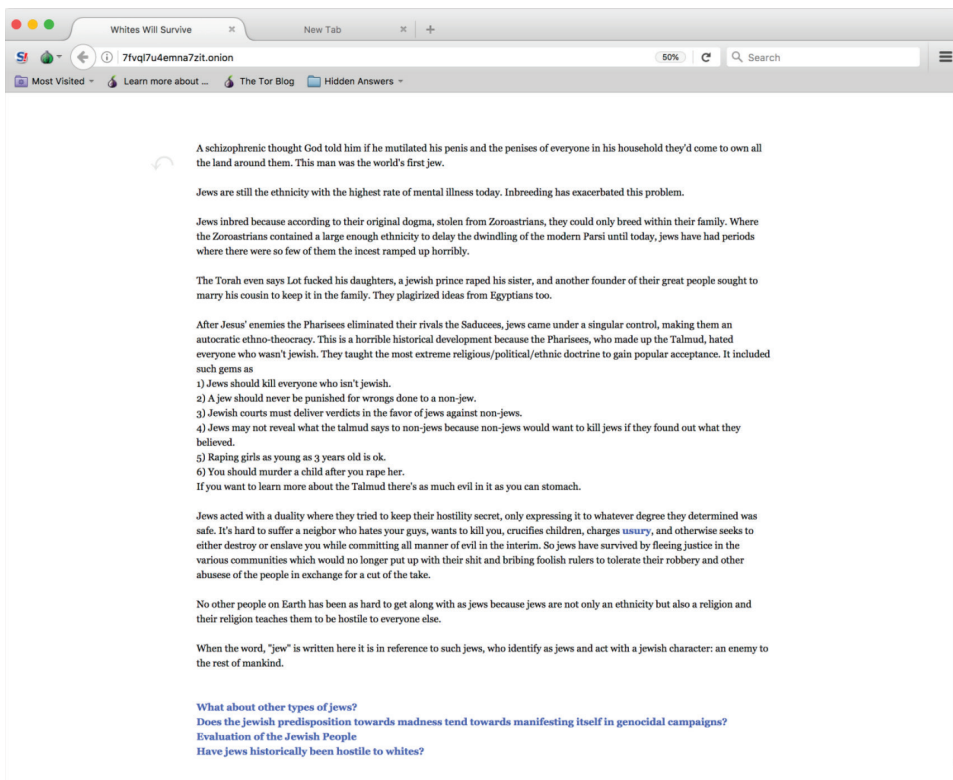


FIGURE 3. *White Will Survive* (Blog), description of Jews.

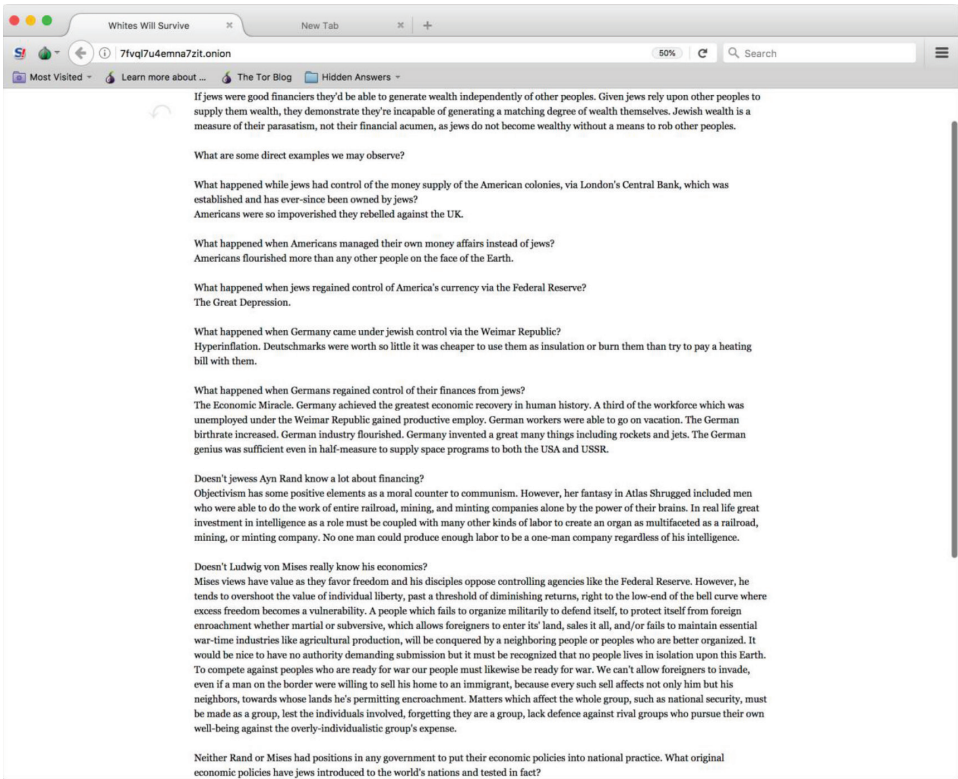


FIGURE 4. *White Will Survive* (Blog), Jews and money.

difference is that surface web users can be easily held accountable for their content. For instance, Gareth Wardell, a Scottish National Party (SNP) supporter and the publisher of the *Grouse Beater* (Blog)⁸² was suspended from party membership in late 2018 for citing *Mein Kampf* in an attack against a Jewish Labour party activist.⁸³

Forums and Boards

Forums and boards on the dark web are similar to their parallels on the surface web. One can start a discussion, topic, or a question by simply publishing it for all users to see. Searching for “Nazi,” “Jews,” “White,” and various other antisemitic and race-related terms gives interesting and troubling results. For example, antisemites frequently use the board of *Hidden*

Answers (Blog) to research antisemitism and racism, Holocaust denial and Nazi propaganda. In moments, one can find the following posts and questions:

“Is it legit to make a videogame where the main objective is to kill jews.”⁸⁴

“Where can I buy authentic nazi memorabilia.”⁸⁵

“Things about Nazi (Hitler), Some one has any link in DW that says things about Nazis?.”⁸⁶

“How come that jews run the U.S. Federal Reserve System (FED) for ~100 yrs?”⁸⁷

“How much money (\$ billions) did the jews made from the Holohoax?”⁸⁸

“Should all jews outside of Israel be killed? [poll].”⁸⁹

“Are the Zionists the Illuminati?”⁹⁰

“Did hitler really kill 6 million jews?”⁹¹

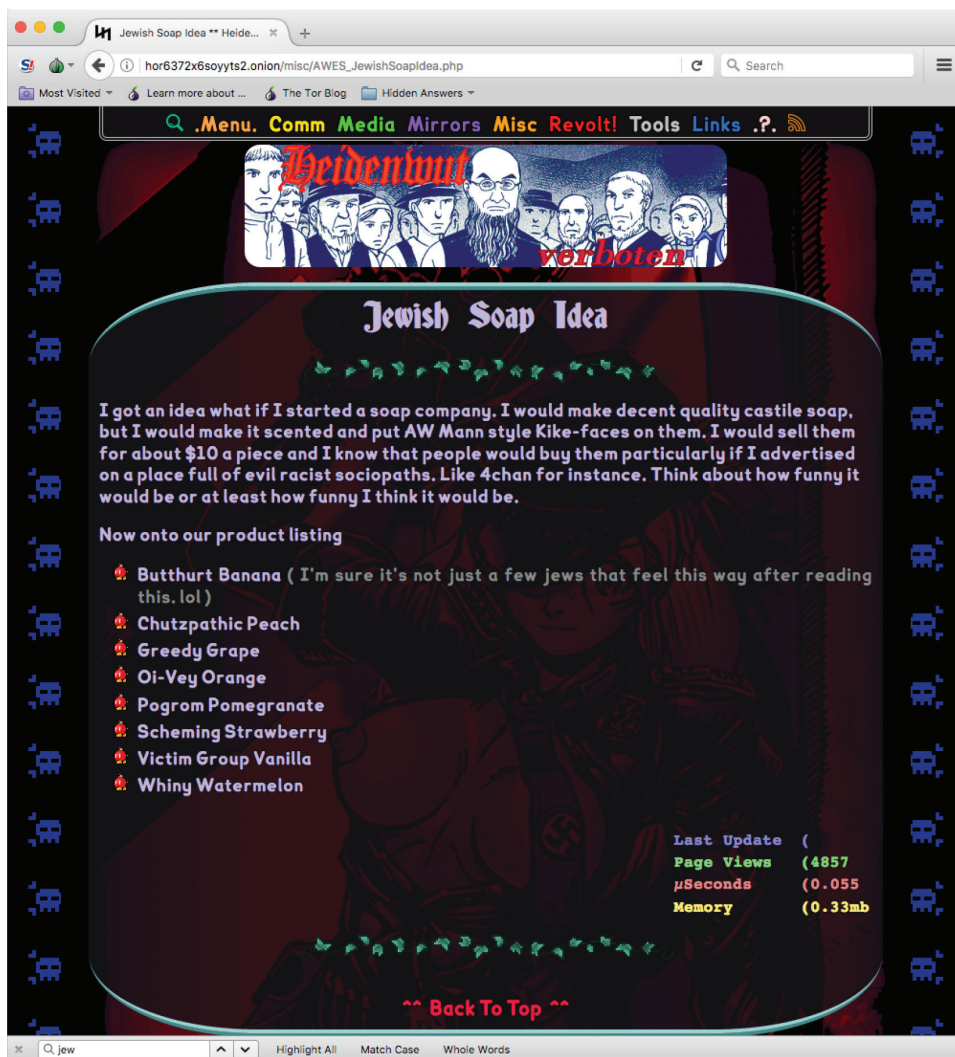


FIGURE 5. *Heidenwut* (Blog), Jewish Soap Idea.

Another alarming example is a forum which disguises itself as a credible source for intelligence and information—IntelExchange.⁹² Only registered members can enter the forum, which has several boards devoted to general discussions, current events, conspiracy theories, and so forth. The top posts include antisemitic and anti-Zionist “plots” to take over countries and world. For instance, there are posts about Jewish and Israeli conspiracies: Jews are behind

assassination plots; Israel and Jews were behind the 9/11 terror attack; Israel and Jews try to attack and suppress Iran; Israel and Jews manipulate and eliminate Gaza and the Palestinians; and other racist conspiracies.⁹³

A well-known racist and antisemitic forum is Politically Incorrect,⁹⁴ where users discuss various issues in a racist manner. In some discussions and posts, users ask for “Jew-free” versions of platforms, say that Jews are terrorists

and plotters, and use many other antisemitic tropes. Another site is Kiwi Farms,⁹⁵ where a simple search of the term “Jews” will bring up various antisemitic and anti-Zionist themes. Other forums and boards include Raddle,⁹⁶ Endchan,⁹⁷ The Stock Insiders,⁹⁸ OnionLand,⁹⁹ and *Скрытые Ответы* (the Russian *Hidden Answers* [Blog]).¹⁰⁰

Unlike the *Daily Stormer*, these sites and forums will not be taken down easily as they are not controlled by big tech companies, ICANN, or other regulators. If they are taken offline by white-hat hackers¹⁰¹ or by a governmental operation (US or Israeli, for example), they will simply rise online again with a different domain or a different site design. Furthermore, since these sites are not indexed by regulated services, it will be a long time until liberal societies can trace new antisemitic sites and fight them. It is important to note that surface web forums and boards such as 4chan¹⁰² are also used for racist rhetoric and are seldom regulated. Unless they are on dedicated antisemitic sites, surface web uses often oppose expressions of racism and comment against antisemitic posts.

Social Networks

Social Networks on the dark web are similar to surface web networks such as Facebook, Twitter, LinkedIn, Google+, or Gab. As with surface web services, a user can join a specific social network on the dark web and create a profile. Once a profile is created, posts, stories, pictures, and videos can be uploaded to present the user or his ideas.

In August 2018, the surface web social network Gab,¹⁰³ hosted by Microsoft, was notified by a third party that some controversial antisemitic posts saying Jews should be raised as livestock were uploaded on the platform and were being spread. Microsoft imposed a call for action on Gab and gave it forty-eight hours to remove all antisemitic posts. If Gab failed to act, Microsoft would stop the hosting the site and it would likely be offline for months.¹⁰⁴

After restrictions and bans on the surface web, alt-right antisemites go to dark web social networks to manifest their extreme ideologies. The dark web has a few popular social networks for antisemites to thrive in: Connect,¹⁰⁵ Galaxy3,¹⁰⁶ Torbook,¹⁰⁷ for example. There is even a dark web Facebook.¹⁰⁸ For the Connect social network, what matters most is privacy and nothing else: “You want an account with Connect? The reason is that your privacy matters a lot to you and you would like an account that is disconnected from your official identity? This is absolutely reasonable.”¹⁰⁹

Once inside a dark web social network, in this case Connect, a variety of pages, users, and posts can be found.¹¹⁰ For example, annalolita (who also posts a lot of sexual material), frequently publishes conspiracy theories alongside antisemitic tropes. An illustration from August 11, 2018 claims “the Rothschilds” and other Jews control the US government and world finance and banking services—a classical anti-Semitic stereotype.¹¹¹

Other profiles on the dark web post antisemitic and anti-Zionist tropes, illustrations, and conspiracy theories. Most state that Israel and the Jewish people govern the world by means of money and corruption.¹¹² However, it is important to note that antisemitic groups and pages on surface web social media are common as well. In a simple search on Facebook for the words “Holocaust lies,” “Jews,” and “Zionists,” one can find pages titled “Holocaust was a lie,”¹¹³ “Zionists Crimes Exposed,”¹¹⁴ and many others. A recent newspaper report lists material designed to “incite hatred and violence against Jews.”¹¹⁵

CONCLUSION

This article has examined racism and antisemitism on the deep web and the dark web, and developed a new conceptual framework—that is, a toolset—for further social science research on the subject. The key rationale behind this research is fairly simple. If racism

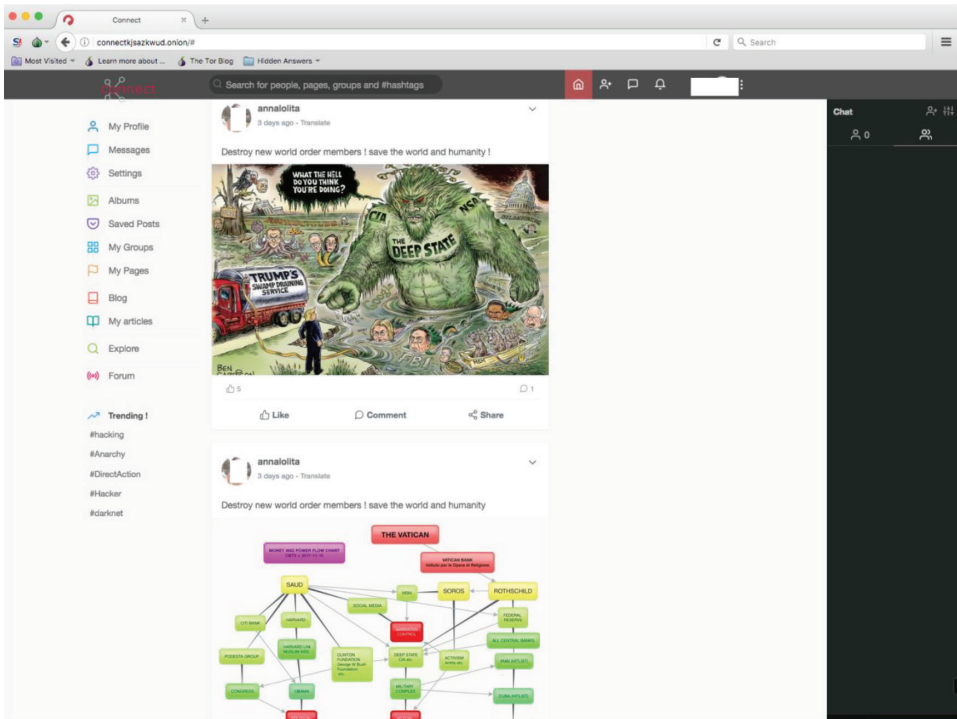


FIGURE 6. Annalolita, conspiracy and anti-semitic illustrations.

and antisemitism are not accepted by modern liberal societies, antisemites will find shelter on the outskirts of society. In the same way that crime happens in alleyways at night, hidden from view, racism lives in the hidden away, digital crevices—in the dark web.

Antisemitism on the dark web is found among white supremacy groups, neo-Nazis, and other kinds of nationalists. In addition, some extreme Islamists also use antisemitism and anti-Zionism to spread hatred. Interestingly, the left kind of antisemitism mentioned in the conceptual framework of this article does not have a significant footprint on the dark web. This fact proves my argument that left antisemitism is still socially acceptable. Right-wing antisemitism is not accepted and thus it inhabits the fringes of society. Left antisemitism, on the other hand, presenting itself as a critique of Israeli policies, does not have to hide on the

dark web. Society finds its (disguised) antisemitism acceptable.

Several of the dark web platforms and sites of most interest to social scientists were presented and compared to their surface web equivalents. They were selected in order to describe, and demonstrate empirically, the prevalence of antisemitism on the dark web: marketplaces which sell antisemitic and Nazi items; blogs which provide antisemites with an anonymous platform to spread hate; obscene forums and boards; and social sites on which users share antisemitic ideas and talk about Jew-hatred publicly (but, due to the nature of the dark web, effectively in private). Sites which were banned by society, such as the *Daily Stormer*, find shelter in the unregulated world of the dark web.

Unfortunately, contemporary liberal society has not eradicated antisemitism. Governments are not taking sufficient action to combat

antisemitism online. Moreover, attempts to ban it from the surface web—which is only five to ten percent of the web as a whole—force antisemites underground and onto the almost immeasurable dark web. Thus, society actually enables antisemites to spread their hatred and thrive. The main applicable contribution of this paper is the fact that it presents as ancient phenomenon on very contemporary platforms such as the dark web. In addition, methods and ideas of exploration can benefit

others in their research of the platforms, not only about antisemitism but in general social trends.

Future research can study the dark web through systematic analyses of antisemitic trends on each of the social platforms discussed above, dark web heuristics, or the use of AI and other monitoring and mapping tools. The only dark web platform presented in this article was TOR: Future research can explore other dark webs such as Freenet, I2P, and Riffle.

REFERENCES

- Gabrielle Berman and Paradies Yin, "Racism, Disadvantage and Multiculturalism: Towards Effective Anti-Racist Praxis," *Ethnic and Racial Studies* 33, no. 2 (2008): 214-232.
- Lev Topor, "Explanations of Antisemitism in the British Postcolonial Left," *Journal of Contemporary Antisemitism* 1, no. 2 (2018): 1-14.
- Phyllis B. Gerstenfeld, Diana R. Grant, and Chau-Pu Chiang, "Hate Online: A Content Analysis of Extremist Internet Sites," *Analyses of Social Issues and Public Policy* 3, no. 1 (2003): 29-44.
- Robert S. Wistrich, "Gaza, Hamas, and the Return of Antisemitism," *Israel Journal of Foreign Affairs* 8, no. 3 (2014): 35-48.
- Norman Geras, "Alibi Antisemitism," *fathom*, Spring 2013, <http://fathomjournal.org/alibi-antisemitism/>.
- Alex Hern, "The Dilemma of the Dark Web: Protecting Neo-Nazis and Dissidents Alike," *The Guardian*, August 23, 2017, <https://www.theguardian.com/technology/2017/aug/23/dark-web-neo-nazis-tor-dissidents-white-supremacists-criminals-paedophile-rings/>.
- Dakota S. Rudesill, James Caverlee, and Daniel Sui, *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box* (2015), accessed July 11, 2018, <https://www.wilsoncenter.org/publication/the-deep-web-and-the-darknet>.
- Andre Oboler, "Online Antisemitism 2.0. 'Social Antisemitism' on the 'Social Web,'" *Jerusalem Center for Public Affairs*, accessed December 4, 2018, <http://jcpa.org/article/online-antisemitism-2-0-social-antisemitism-on-the-social-web/>; Andre Oboler, "The Normalization of Islamophobia through Social Media: Facebook," in *Islamophobia in Cyberspace*, ed. Imran Awan, (London: Routledge, 2016), 41-63.
- John Eck and L. Weisburd David, "Crime Places in Crime Theory," *Crime and Place: Crime Prevention Studies*, 4: 1-33; Hebrew University of Jerusalem Legal Research Paper. Available at SSRN: <https://ssrn.com/abstract=2629856>
- George Hurlburt, "Shining Light on the Dark Web," *IEEE Computer* 50, no. 4 (2017): 100-105.
- Ciancaglini, Balduzzi, Goncharov, and McArdle, "Deepweb and Cybercrime."
- ICANN.org, accessed July 19, 2018, <https://www.icann.org/>.
- "About Google Services," accessed July 20, 2018, <https://www.google.com/about/our-company/>.
- Lucas D. Introna and Helen Nissenbaum, "Shaping the Web: Why the Politics of Search Engines Matters," *The Information Society* 16, no. 3 (2000): 169-185.
- Mary-Ann Russon, "Won't Let Your Citizens Access the Internet? Fine, No More IP Addresses for You," *International Business Times*, April 21, 2017, <https://www.ibtimes.co.uk/wont-let-your-citizens-access-internet-fine-no-more-ip-addresses-you-1618040/>; Sophia Dastagir Vogt, "The Digital Underworld: Combating Crime on the Dark Web in the Modern Era," *Santa Clara Journal of International Law* 15 (2017): 104-125.
- Bahrain Watch Members, "The IP Spy Files—How Bahrain's Government Silences Anonymous Online Dissent," *Bahrain Watch* (2013), accessed July 24, 2018: <https://bahrainwatch.org/ipspy/>.

- 17 Michel Foucault, *Society Must Be Defended: Lectures at the Collège de France, 1975–76*, trans. David Macey (New York: Picador, 2003), 43–62.
- 18 Lev Topor, "Dark and Deep Webs: Liberty or Abuse," *International Journal of Cyber Warfare and Terrorism* 9, no. 2 (2019): 1–14.
- 19 George Hurlburt, "Shining Light on the Dark Web," 100–105.
- 20 Introna, Lucas D., and Helen Nissenbaum. "Shaping the Web: Why the politics of search engines matters," *The Information Society* 16, no. 3 (2000): 169–185; Eszter Hargittai, "The Social, Political, Economic, and Cultural Dimensions of Search Engines: An Introduction," *Journal of Computer-Mediated Communication* 12, no. 3 (2007): 769–777.
- 21 TOR, the Onion router, is explained (and available) here: <https://www.torproject.org/about/history/>.
- 22 See George Hurlburt, "Shining Light on the Dark Web," 100–105; Ciancaglini, Balduzzi, Max Goncharov, and Robert McArdle, "Deepweb and Cybercrime."
- 23 Ibid.
- 24 Shahzeb Ali Rathore, "Deep Web: The 'Dark' Side of IS," *RSIS Commentaries*, No. 275, (2016), <https://dr.ntu.edu.sg/bitstream/handle/10220/41704/CO16275.pdf?sequence=1>; George Hurlburt, "Shining Light on the Dark Web," 100–105.
- 25 The TOR project is mostly funded by the US Government. In 2013, the US National Science Foundation, along with some universities, gave \$1.8 million to the project. See <https://www.torproject.org/about/sponsors.html.en/>.
- 26 Ciancaglini, Balduzzi, Goncharov, and McArdle, "Deepweb and Cybercrime."; Eric Jardine, "The Dark Web Dilemma: Tor, Anonymity and Online Policing," *Global Commission on Internet Governance* (2015), accessed July 27, 2018: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2667711.
- 27 Ibid.
- 28 Lev Topor, "Dark and Deep Webs: Liberty or Abuse," 1–14.
- 29 Ciancaglini, Balduzzi, Goncharov, and McArdle, "Deepweb and Cybercrime."; Hsinchun Chen, Wingyan Chung, Jialun Qin, Edna Reid, Marc Sageman, and Gabriel Weimann, "Uncovering the Dark Web: A Case Study of Jihad on the Web," *Journal of the American Society for Information Science and Technology* 59, no. 8 (2008): 1347–1359.
- 30 Thomas Fox-Brewster, "Memex in Action: Watch DARPA Artificial Intelligence Search For Crime On The 'Dark Web,'" *Forbes*, April 10, 2015, <https://www.forbes.com/sites/thomasbrewster/2015/04/10/darpa-memex-search-going-open-source-check-it-out/>.
- 31 Massimo La Morgia, Alessandro Mei, Simone Raponi, and Julinda Stefa, "Time-Zone Geolocation of Crowds in the Dark Web" (presentation, IEEE International Conference on Distributed Computing Systems [ICDCS], Vienna, Austria, 2–6 July, 2018).
- 32 Flora Nathaniel, "How to Safely Browse the Deep Web," Lifehack.org, accessed August 2, 2018, <https://www.lifehack.org/534109/how-safely-browse-the-deep-web/>.
- 33 George Hurlburt, "Shining Light on the Dark Web," 100–105.
- 34 Robert W. Gehl, "Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network," *New Media & Society* 18, no. 7 (2016): 1219–1235.
- 35 Anol Bhattacharjee, Social Science Research: Principles, Methods, and Practices, *Textbooks Collection* 3 (2012): 73–103.
- 36 "The Hidden Wiki", accessed August 1, 2018, http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page. Please note: Access cannot be gained without an Onion (TOR) browser.
- 37 Ahmia.fi search engine for .onion sites, accessed August 1, 2018, <https://ahmia.fi/>.
- 38 Torch search engine for .onion sites, accessed August 1, 2018, <http://xmh57jrznw6insl.onion/>.
- 39 The fascist activist who drove the car into the crowded demonstration in Charlottesville, causing the death of Heather Heyer, was convicted of first-degree murder sixteen months after the event. See Jonathan M. Katz and Farah Stockman, "James Fields Guilty of First-Degree Murder in Death of Heather Heyer," *The New York Times*, December 7, 2018, <https://www.nytimes.com/2018/12/07/us/james-fields-trial-charlottesville-verdict.html>.
- 40 *The Daily Stormer* is described and analyzed in Luke O'Brien, "The Making of American Nazi," *The Atlantic*, December 2017, <https://www.theatlantic.com/magazine/archive/2017/12/the-making-of-an-american-nazi/544119/>.
- 41 *The Daily Stormer's* new online website and blog is at <https://dstormer6em3i4km.onion.link>.

- 42 Vincenzo Ciancaglini, Marco Balduzzi, Max Goncharov, and Robert McArdle, *Deepweb and Cybercrime, Trend Micro Report* 9 (2013): 5-6, accessed July 13, 2018: <https://www.trendmicro.ae/media/wp/deepweb-and-cyber-crime-whitepaper-en.pdf>; Adi Robertson, "Neo-Nazi Site Moves to Dark Web after GoDaddy and Google Bans," *The Verge*, August 15, 2017, <https://www.theverge.com/2017/8/15/16150668/daily-stormer-alt-right-dark-web-site-godaddy-google-ban/>.
- 43 Kelly Heather, "Hate Groups on Facebook: Why Some Get to Stay," CNN.com, accessed December 4, 2018, <https://money.cnn.com/2017/08/17/technology/culture/facebook-hate-groups/index.html>.
- 44 Rebecca MacKinnon, Elonnai Hickok, Allon Bar, and Hae-in Lim, *Fostering Freedom Online: The Role of Internet Intermediaries*, UNESCO Publishing (Paris: UNESCO, 2015), https://repository.upenn.edu/cgi/viewcontent.cgi?article=1000&context=cgcs_publications; Paulina Wu, "Impossible to Regulate? Social Media, Terrorists, and the Role for the UN," *Chicago Journal of International Law* 16, no. 1 (2015): 281-311.
- 45 Stormfront.org, accessed October 26, 2018, <https://www.stormfront.org/forum/index.php>.
- 46 Jewwatch.com was active until the end of 2018. The site is offline due to complaints to its internet providers and regulators. The site was banned and sanctioned many times, it changed its IP address 37 times and changed to 13 unique names 15 times in the last 15 years.
- 47 Alex Hern, "Stormfront: 'Murder Capital of Internet' Pulled Offline after Civil Rights Action," *The Guardian*, August 29, 2017, <https://www.theguardian.com/technology/2017/aug/29/stormfront-neo-nazi-hate-site-murder-internet-pulled-offline-web-com-civil-rights-action>.
- 48 Andre Oboler, *Measuring the Hate: The State of Antisemitism in Social Media*, Online Hate Prevention Institute (Melbourne: Online Hate Prevention Institute, 2016), <http://mfa.gov.il/MFA/ForeignPolicy/AntiSemitism/Documents/Measuring-the-Hate.pdf>.
- 49 "German Prosecutors Investigate Facebook Over Hate Posting," *Reuters*, November 4, 2016, <https://www.reuters.com/article/us-germany-facebook/german-prosecutors-investigate-facebook-over-hate-postings-idUSKBN12Z2BI>.
- 50 *Anti-Semitic Symbols and Holocaust Denial in Social Media Posts—January 2018*, World Jewish Congress and Vigo Social Intelligence (World Jewish Congress, 2018), <http://www.worldjewishcongress.org/download/3KVjY-gi8FN0tdWd5HeFPw>.
- 51 Samuel Woolley, *Computational Propaganda, Jewish-Americans and the 2018 Midterms: The Amplification of Anti-Semitic Harassment Online*, ADL (New York: ADL, 2018), <https://www.adl.org/media/12028/download>.
- 52 "Hate Crime Statistics, 2017," Federal Bureau of Investigation, <https://ucr.fbi.gov/hate-crime/2017/topic-pages/incidents-and-offenses>.
- 53 Dakin Andone, "A Year After Charlottesville, Washington Braces for Another White Nationalist Protest," CNN.com, accessed August 12, 2018, <https://www.cnn.com/2018/08/12/us/unite-the-right-charlottesville-anniversary/index.html>.
- 54 Edward G. White, "The First Amendment Comes of Age: The Emergence of Free Speech in Twentieth-Century America," *Michigan Law Review* 95, no. 2 (1996): 299-392.
- 55 P. R. Lockhart, "The Alt-Right Is Coming to Washington, DC. Here's How Anti-Racist Groups Are Preparing," *VOX*, August 12, 2018, <https://www.vox.com/identities/2018/8/6/17653252/unite-the-right-2018-counterprotest-anti-racist-washington-dc>.
- 56 *Daily Stormer*, "Surface Web New Domain," accessed August 13, 2018, <https://dailystormer.name/>.
- 57 *Daily Stormer*, "Current Status: UP," accessed August 10, 2018, <http://dstormer6em3i4km.onion/>.
- 58 Andrew Anglin, "Live Thread: DC 'Unite the Right 2' Rally," *Daily Stormer*, August 12, 2018, <https://dailystormer.name/live-thread-dc-unite-the-right-2-rally/>.
- 59 Heather Heyer, the victim of the 2017 Unite the Right rally, was shamelessly and hatefully depicted in the *Daily Stormer* a day after the 2018 rally. The words and illustrations are not presented in this article due to their shocking nature. See Joe Isolated, "Memetic Monday: THOTS, Nogs, and ZOG," *Daily Stormer*, August 13, 2018, <https://dailystormer.name/memetic-monday-thots-nogs-and-zog/>.
- 60 Lev Topor, "Explanations of Antisemitism in the British Postcolonial Left," *Journal of Contemporary Antisemitism* 1, no. 2 (2018): 1-14.
- 61 Michal-Hatuel Radoshitzky, "Containing the Link Between BDS and Anti-Semitism," *Jerusalem Post*, June 3, 2015, <https://www.jpost.com/Opinion/Containing-the-link-between-BDS-and-anti-Semitism-404964/>.

- 62 David Hirsh, "Hostility to Israel and Antisemitism: Towards a Sociological Approach," *Journal for the study of Antisemitism* 5 (2013): 1401-1422; Eve Garrard, "Anti-Judaism, Anti-Zionism, Antisemitism," *fathom*, Winter, 2015, <http://fathomjournal.org/anti-judaism-anti-zionism-antisemitism/>.
- 63 Hamed Abdel-Samad, *Islamic Fascism* (Amherst: Prometheus Books, 2016), 9-14, 15-23, 193-206; Michael Berenbaum, *Not Your Father's Antisemitism: Hatred of the Jews in the Twenty-First Century* (Minnesota: Paragon House Publishers, 2008), 101-117.
- 64 Ciancaglini, Balduzzi, Goncharov, and McArdle, "Deepweb and Cybercrime."
- 65 Eva Kaján, "Hate Online: Anti-Immigration Rhetoric in Darknet," *Nordia Geographical Publications* 46, no. 3 (2017): 3-22.
- 66 Rudesill, Caverlee, and Sui, "The Deep Web and the Darknet."
- 67 Ibid.
- 68 Note that many of the dark web sites, domains, and designs are frequently changed and/or removed, and that they may be inaccessible in the future as a site or archive.
- 69 Julia Buxton and Tim Bingham, "The Rise and Challenge of Dark Net Drug Markets," *Policy Brief* 7 (2015).
- 70 "First Nationwide Undercover Operation Targeting Darknet Vendors Results in Arrests of More Than 35 Individuals Selling Illicit Goods and the Seizure of Weapons, Drugs and More Than \$23.6 Million," justice.gov, accessed August 5, 2018, <https://www.justice.gov/opa/pr/first-nationwide-undercover-operation-targeting-darknet-vendors-results-arrests-more-35>.
- 71 Valhalla, accessed August 5, 2018, <http://valhallaxmn3fydu.onion/register/DpXB>.
- 72 Imperial Library, accessed August 5, 2018, <http://xfrmro77i3lixucja.onion/>.
- 73 Dream Market, accessed August 5, 2018: <http://vzatgqjilebaxluc.onion/>.
- 74 Hitler's *Mein Kampf* is banned in its original form in Germany, Poland, and other European countries. See Felicity Capon and Scott Catherine, "Top 20 Books They Tried to Ban," *The Telegraph*, October 20, 2014, <https://www.telegraph.co.uk/culture/books/booknews/9900733/Top-20-books-they-tried-to-ban.html>. For a web-based version of *Mein Kampf* on the .onion platform, see <http://rqkz2zcavqlzu32e.onion/mein%20Kampf/>.
- 75 *The Protocols of the Elders of Zion*, and other Nazi-related propaganda materials, can also be found on the surface web, but there is usually a warning attached. In the text for sale on Amazon, a warning by the Anti-Defamation League declares the document's highly racist nature. See https://www.amazon.com/Protocols-Learned-Elders-Zion/dp/1981685693/ref=sr_1_1?ie=UTF8&qid=1540385681&sr=8-1&keywords=protocols+of+the+elders+of+zion&dpID=41V3qN7AimL&preST=_SY344_BO1,204,203,200_QL70_&dpSrc=srch. "Russian Academicians Demand Ban of Protocols of the Elders of Zion," rt.com, accessed September 11, 2019, <https://www.rt.com/politics/academicians-demand-elders-zion/>.
- 76 Brian Bergstein, "Ebay Bans Nazi Hate Material," *ABC News*, accessed September 25, 2019, <https://abcnews.go.com/amp/Technology/story?id=98593&page=1>
- 77 Lindsay Isaac, "Ebay Removes Purported Holocaust Memorabilia from Site, Apologizes," CNN.com, accessed August 6, 2018, <https://edition.cnn.com/2013/11/03/world/ebay-holocaust-memorabilia/index.html>.
- 78 "Amazon Removes Nazi-Themed Items After Complaints," *The Associated Press*, accessed September 25, 2019, <https://www.apnews.com/4b55c31afb174d218e768305f91a554f>
- 79 *White Will Survive* (Blog), accessed August 11, 2018, <http://7fvql7u4emna7zit.onion/>.
- 80 *Heidenwut* (Blog), accessed August 11, 2018, <http://hor6372x6soyyts2.onion/blog/000i.php>.
- 81 "The Shutting," *Heidenwut* (Blog), accessed August 10, 2018, http://hor6372x6soyyts2.onion/blog/2017_01_12.php.
- 82 *For Grouse Beater* (Blog), see <https://grousebeater.wordpress.com>.
- 83 Tom Gordon, "SNP suspends member over Anti-Semitic Blog," *The Herald*, October 30, 2018, <https://www.herald-scotland.com/news/17188323.snp-suspends-member-over-anti-semitic-blog/>.
- 84 "answeranswer," accessed August 9, 2018, <http://answerstedhtcbek.onion/125331/is-it-legit-make-videogame-where-the-main-objective-kill-jews?show=125331#q125331>.
- 85 "Markscln," accessed August 9, 2018, <http://answerstedhtcbek.onion/173608/wher-can-i-buy-authentic-nazi-memorabilia?show=173608#q173608>.
- 86 "VPM," accessed August 9, 2018, <http://answerstedhtcbek.onion/137555/things-about-nazi-hitler?show=137555#q137555>.

- 87 Search Results for the “Jews” on *Hidden Answers* (Blog), accessed August 10, 2018, <http://answerstedhctbek.onion/search?q=jews>.
- 88 Ibid.
- 89 Ibid.
- 90 Ibid.
- 91 Ibid.
- 92 *IntelExchange*, accessed August 10, 2018, <http://rrcc5uu3dkhlvdwo.onion/>.
- 93 “Current events,” *The Conspiracy*, accessed August 10, 2018, <http://rrcc5uu3dkhlvdwo.onion/?cmd=category&id=2>, <http://rrcc5uu3dkhlvdwo.onion/?cmd=category&id=3>.
- 94 *Politically Incorrect*, accessed August 10, 2018, <http://endchan5dovxprs5.onion/pol/>.
- 95 *Kiwi Farms*, accessed August 10, 2018, <http://kiwifarms6v775u6.onion/>.
- 96 *Raddle*, accessed August 12, 2018, <http://lfbg75wjgi4nzdio.onion/>.
- 97 *Endchan*, accessed August 12, 2018, <http://s6424n4x4bsmq527.onion/>.
- 98 *Stock Insiders*, accessed August 10, 2018, <http://b34xhb2kf3nbuyk.onion/index.php>.
- 99 *OnionLand*, accessed August 10, 2018, <http://onionlandbakyt3j.onion/>.
- 100 *Скрытые Ответы*, accessed August 10, 2018, <http://kdrxcxan24rxglcy.onion/>.
- 101 White-hat hackers find flaws in systems for two reasons: 1. To help fix and strengthen a site; 2. To hack a malicious site, such as one run by a terrorist or racist group, and stop it functioning.
- 102 4chan bulletin board, accessed November 28, 2018, <https://www.4chan.org>.
- 103 Gab.ai is a popular social network within the white supremacy and alt-right community. The platform describes itself as “The Free Speech Social Network.” Following a BBC investigation, Gab.ai became a go-to network for extreme groups and fascists. See “Gab: Free Speech Haven or Alt-Right Safe Place?” BBC.com, accessed August 14, 2018, <https://www.bbc.com/news/blogs-trending-38305402>.
- 104 James Cook, “Anti-Semitic Posts Deleted from ‘Alt-Right Social Network’ Following Microsoft Crackdown,” *The Telegraph*, August 10, 2018, <https://www.telegraph.co.uk/technology/2018/08/10/anti-semitic-posts-deleted-alt-right-social-network-following/>.
- 105 Connect, accessed August 14, 2018, <http://connectkjsazkwud.onion/>.
- 106 Galaxy3, accessed August 14, 2018, <http://galaxy3m2mn5iqtn.onion/>.
- 107 Torbook, accessed August 14, 2018, <http://injj4qvzyun6zq3a.onion/>.
- 108 Dark Web Facebook, accessed August 14, 2018, <https://www.facebookcorewwi.onion/>.
- 109 “Terms of Use,” Connect, accessed August 14, 2018, <http://connectkjsazkwud.onion/terms/terms>.
- 110 A fake Connect user profile was created and managed specifically for this research.
- 111 Connect does not provide usable links to profiles. Rather, it uses the same link to all profiles—<http://connectkjsazkwud.onion/#>.
- 112 Ibid.
- 113 “Holocaust was a Lie,” Facebook, accessed November 27, 2018, <https://www.facebook.com/groups/185009615299922/>.
- 114 “Zionists Crimes Exposed,” Facebook, accessed November 27, 2018: <https://www.facebook.com/groups/623043274491450/>.
- 115 Katie Gibbons, “Antisemitic Hate Posts Allowed by Facebook,” *The Times*, July 27, 2018, <https://www.thetimes.co.uk/edition/news/antisemitic-hate-posts-including-holocaust-denial-allowed-by-facebook-7crdvwc2x>.