

ISD

Institute
for Strategic
Dialogue

GDI

Global
Disinformation
Index

The Business of Hate

Bankrolling Bigotry in Germany
and the Online Funding of Hate Groups

POLIZEI

POLIZEI

Nationale Sozialisten
Rhein-Neckar

Note

All data on the online funding services on the websites of the actors are as of September 2-10, 2021. Screenshots of the websites or social media profiles for all analyzed data are available upon request. All policies (“Terms of Service”) of the online funding services are saved in the Wayback Machine on September 10, 2021. Websites are not named or linked to in order to avoid attracting additional visitors to them. However, the URLs of these websites can be provided upon request.

After publication, a spokesperson of Automattic, the company that owns WooCommerce and WordPress.com, contacted ISD to clarify the status of WooCommerce as an open-source product that anyone can install on their own servers. If the WooCommerce product is self-hosted, Automattic currently has no means of enforcing its user guidelines to limit the use of its product, even if it is being used by hate groups. Our own verification process could not find any indication that any of the websites mentioned in the report are hosted on Automattic servers. Further information on reporting content on a store built with WooCommerce, and Automattic’s ability to take action, can be found [here](#). Aside from the open-source WooCommerce product, Automattic offers a payment service in the form of WooCommerce Payments. If a site is using WooCommerce Payments, Automattic has the ability to enforce its terms of service (TOS) directly and block users from using their service. However, none of the actors listed in this report were clients of this service at the time of writing the report.

The use of open-source software like WooCommerce and WordPress by extremists and hate groups is widespread - not just in Germany. The challenges and opportunities of this phenomenon are further explored in our recently published report [Open Source, Self Defence: Tackling the Challenge of Extremist Websites and Open Source Tech](#).



Beirut | Berlin | London | Paris | Washington DC

Copyright © Institute for Strategic Dialogue (2020). Institute for Strategic Dialogue (ISD) is a company limited by guarantee, registered office address PO Box 75769, London, SW1P 9ER. ISD is registered in England with company registration number 06581421 and registered charity number 1141069. All Rights Reserved.

www.isdglobal.org



The Global Disinformation Index is a UK-based not-for-profit that operates on the three principles of neutrality, independence and transparency. Our vision is a world in which we can trust what we see in the media. Our mission is to restore trust in the media by providing real-time automated risk ratings of the world’s media sites through a Global Disinformation Index (GDI). The GDI is non-political. Our Advisory Panel consists of international experts in disinformation, indices and technology.

For more information, visit www.disinformationindex.org

Executive Summary

Hate crime is on the rise in Germany. According to the latest report by the Ministry of the Interior and the Federal Criminal Police Office, the cases of politically motivated crime rose by nearly 20 percent in 2020.¹ Of the more than 10,000 recorded hate crimes in 2020, over 80 percent were classified as 'right-wing'. The rise in hate crime goes hand-in-hand with the proliferation of a plethora of right-wing extremist entities, including organisations, parties and individuals. Much attention has been paid to how these entities levy the powers of the internet and social media to spread their hate. But not enough focus has been placed on the online funding services which enable these groups to fund themselves.

The Global Disinformation Index (GDI) and the Institute for Strategic Dialogue (ISD) have conducted a study on the different online services that German extremists allegedly use to raise funds, the findings of which are presented in this summary briefing. The study puts a spotlight on these online funding channels and how they are used to finance these organisations. This analysis builds on a methodology deployed in a 2020 joint study on the use of online funding services by U.S. hate groups.²

Our German research focused on 17 suspected right-wing extremist groups and entities in Germany.³ These groups include political parties, news sites, publishers, associations, and organisations, as well as prominent individuals within Germany's extremist movement. The groups' ideological spectrum ranges from national socialism to the 'new right', from ethnonationalism to conspiracy theorist sovereigntists. All groups and entities analysed in this report are currently being observed by Germany's domestic intelligence body, have material links to these groups⁴, or have been indicted for allegedly inciting hatred.⁵

This study shows that these right-wing extremist organisations allegedly use 20 different online funding services to raise funds (see Table 1). Ultimately, the research uncovered 79 documented instances of extremist organisations using various well-known online fundraising services, among them PayPal, WooCommerce and Square, to support their activity.

Further analysis indicates that 12 of these services have explicit policies prohibiting the use of their platforms for the promotion of hate or violence (see Table 2). This suggests that there is allegedly a significant enforcement gap in Germany. This also demonstrates the broader need for online funding services without explicit policies to adopt more robust ToS to prevent extremist movements or actors from using them to fund the spread of hate speech, disinformation, and conspiracy narratives.⁶

Such a policy gap can have significant consequences for a country's social and political processes. These 20 online funding services contribute to the ability of the analysed groups and individuals to spread their agenda ahead of Germany's federal elections.⁷ Many of these groups are leading disinformation campaigns that attack and defame political opponents as well as undermine public confidence in the integrity of Germany's electoral process. Examples from the US and other countries show that the seeding of disinformation narratives online allows such groups to build a broader base of support—in terms of both amplifying their messages and funding their activities.⁸

Documenting the online funding of hate groups is essential, both to hold platforms up to their own standards and to uncover any potential policy gaps which could enable the funding and spread of hatred and social polarisation.

Key findings

Based on the analysis and documentation of these groups' social footprint and online funding services used, we found that:

- **Direct bank transfers are reportedly the most frequently used online funding mechanisms by the German groups investigated.** In this study, 15 out of the 17 entities analysed (88 percent) allegedly use this method to bankroll their activities.
- **WooCommerce (53 percent) is among the most frequently used online payment service providers,** even though the payment platform prohibits this type of activity as outlined in their 'acceptable use' policies against the incitement to violence.⁹
- **Overall, many online funding services were found on these groups' sites despite ToS policies that should have forbidden such activity. These companies include Patreon,¹⁰ Stripe,¹¹ Square,¹² Shopware¹³ and GiveWP.¹⁴** In the case of GiveWP, an online donation plugin, used by the Neo-Nazi Party 'Der III. Weg';¹⁵ the platform's own guidelines are even stated in a 2017 blog post by its CEO that GiveWP does not 'enable hate, discrimination, or violence of any form' (see Table 2).¹⁶
- **Three of these actors (NPD, Uniter, and Frank Kraemer) use Facebook's shop function to sell merchandise.** Overall, a large number of right-wing extremist actors and groups, including the NPD, still have documented and multiple channels on mainstream social media platforms such as Facebook, Instagram, Twitter and YouTube.
- **Online donation appeals are used by some of the actors/groups to support their activities,** even though they do not have non-profit status (which legally turns these 'donations' into 'gifts'). Others have non-profit status despite being listed in reports of Germany's domestic intelligence body (these are mainly parties that are allowed to issue donation receipts). Under German law, tax-free donations can be received only by entities that are recognised by the tax office as 'charitable' organisations that benefit society as a whole.¹⁷
- **Cryptocurrencies** are used by three of the actors: Frank Kraemer accepts Bitcoin and Nikolai Nerling uses Bitcoin and Ether. The Identitäre Bewegung Deutschland uses, according to its own account, the most variety of cryptocurrencies through its website and online shop 'Phalanx Europa', namely Bitcoin, Litecoin, Ripple and Dash.
- **The three groups which are extremist political parties have comparatively limited online funding mechanisms on their own sites.** Die Rechte and Der III. Weg state that they accept bank transfers and use WooCommerce. The NPD uses bank transfers and Gambio. The party with the most diverse set of funding mechanisms is Der III. Weg, which seems to also use Square and GiveWP.
- **These three political parties, however, often run off-site shops or maintain side projects which are used to raise money.** For example, the NPD runs two sites in addition to its official shop, both of which sell merchandise. The NPD also runs 'Deutsche Stimme.' Der III. Weg also runs a shop on a separate website from its main site.

Table 1: Overview of online funding services, by group

Organisation	PayPal	Stripe	Square	Klarna	giroPay	Visa	Mastercard	American Express	Gravity Forms	Cryptowährungen	Banküberweisung	Donorbox	Patreon	DLive	Woo Commerce	Shopware	GiveWP	Western Union	Gambio	Facebook Shops
1 Attila Hildmann	●			●		●	●				●			●						
2 Compact (subscription)	●					●	●	●	●		●				●					
3 Der III Weg (membership)			●								●				●		●			
4 Die Kehre (subscription)	●										●				●					
5 Die Rechte											●				●					
6 Ein Prozent		●			●	●	●	●			●			●		●				
7 Frank Kraemer		●			●	●	●	●		●	●		●			●				●
8 Gefangenenhilfe (donations)															●					
9 Identitäre Bewegung Deutschland (membership)*										●	●					●				
10 Institut für Staatspolitik (donations)											●									
11 Kampf der Nibelungen				●							●				●					
12 Nikolai Nerling		●		●	●	●	●	●		●					●			●		
13 NPD (membership)**	●										●	●							●	●
14 PEGIDA (donation only)	●										●				●					
15 PI News*											●		●							
16 Sven Liebich											●				●					
17 Uniter (donation only)		●									●									●

*Uses Phalanx Europa e-commerce site.

**Includes Deutsche Stimme and Junge Nationalisten (membership)

Table 2: Online funding services: Terms of Service (ToS) and group use

Name of service	ToS on hate groups	Groups using service
Bank transfers	N/A ¹⁸	15
WooCommerce	● Yes ¹⁹	9
Crypto	N/A	3
Paypal	● Yes ²⁰	5
Klarna	N/A ²¹	3
Stripe	● Yes ²²	4
Mastercard	● Partial ²³	5
Shopware	● Yes ²⁴	3
giroPay	● No	3
Gravity Forms	● No	1
Patreon	● Yes ²⁵	2
GiveWP	● Yes ²⁶	1
Donorbox	● Yes ²⁷	1
Facebook-Shops	● Yes ²⁸	3
Visa	● Yes ²⁹	5
American Express	● Yes ³⁰	4
DLive	● Yes ³¹	2
Gambio	● Partial ³²	1
Western Union	● No ³³	1
Square	● Yes ³⁴	1

Recommendations

The findings show that specific actions should be taken to disrupt the online funding channels that, by all appearances, are currently being exploited by these 17 entities. Key recommendations for different stakeholder groups include:

Online funding services and ad tech companies:

- **Enforce Terms of Service decisively and take immediate action when violations occur.** It is clear from the reported findings that there is a pervasive problem of implementation, even for the best intended ToS. There should be easy-to-access mechanisms available to the public to report any such policy violations.
- **Analyse and assess risks how their products could be used** by hate groups in markets outside the U.S., such as Germany. This process should be part of a 'Know Your Customer' approach and should also consider the broader social harms which are enabled if hate groups raise funds through their services.
- **Update Terms of Services when they are in place,** to adequately mitigate against these risks and potential abuses by hate groups. Doing so may be effective in limiting the activity of anti-democratic organisations which seek to degrade and polarise free, fundamental rights-based societies.
- **Align the Terms of Service across similar types of funding services.** The fragmentation of policies means that when one company denies use of its services to a group, it will likely seek out a different company to provide these same services. Greater cross-sector collaboration, such as by setting a 'minimum floor' for the Terms of Service of online funding services, could have a significant impact on extremist activity in Germany as well as internationally.

Banking sector:

- **Conduct risk assessment and due diligence to better understand customers.** Understanding the risk of these groups—in terms of potential exposure to or financing of illegal activities—should be part of a bank's due diligence and regulatory requirements to Know Your Customer (KYC).³⁵
- **De-risk banking clients by removing services to groups that do not meet the risk assessment criteria.** While banks in Germany cannot easily deny services to individuals, they can choose to deny bank accounts to organisations which are not political parties based on an internal risk assessment.³⁶

Conclusion

The findings and recommendations from this report demonstrate the need for a more holistic approach to disrupt the right-wing extremist online ecosystem that is spreading and funding hate. Urgent action is needed to block the monetisation channels that known hate groups in Germany are allegedly using to fund their activities. Given the scale of the problem, the funding of extremist movements should become one of the topics of the upcoming coalition talks. Looking ahead, the EU Digital Services Act (DSA) offers the chance to embed such changes in regulation in Germany and across EU member states.

Annex 1: Methodology & Entity List

The method of analysis involved had two aims:

1. Identify the social media footprint and network of web domains associated with each group.

We looked at each group's digital footprint for presence on Facebook, Twitter, Instagram, YouTube, Reddit, TikTok, Vimeo, Spotify, Telegram, Vkontakte, Bitchute, Gab, Parler, Gettr, Minds, Odysee, and Spreaker.

- In total we identified 299 instances of social accounts linked to these extremist groups across mainstream and fringe social platforms. This included:
 - 89 Twitter accounts, 56 Telegram groups, 48 YouTube channels, 34 Vkontakte groups/pages/accounts, and 26 Facebook groups/pages/accounts³⁷ linked to the groups in our data set.
- All 17 groups had a website, and in two cases they had multiple sites. In general, many of the sites had links to the sites of other groups in the sample.
- This social footprint shows the strong online presence of these extremist groups.

2. Identify the online funding services allegedly being used across their digital footprint.

We deployed different analytical approaches to map potential ties between the groups and online funding mechanisms studied:

- We utilised a combination of advanced web searches as well as Javelin+, a proprietary social listening software tailored to dark social platforms, in order to perform outbound link analysis and identify conversations around fundraising and monetisation strategies. For entities that have websites, the research team analysed the source code to determine whether or not they have embedded indirect payment platforms or ad exchanges on the website.²⁵
- We then manually reviewed the data gathered to identify instances of groups fundraising through their social media activity, removing all false positives from our set.
- We used BuiltWith to view the detailed technology and metadata profiles associated with each group's website to identify every instance of these websites linking to platforms within the categories of onsite retail, flexible fund collection or onsite donation forms.
- Wherever possible, researchers took comprehensive measures to verify that groups were current users of a service.
- However, in rare instances, it may be possible that we captured historical data.

We compiled the data we gathered using the methods outlined above into a unitary dataset, which logged all instances of the hate groups we identified using online funding mechanisms.

The following groups and their referent site(s) are included in this report's analysis. Each of the 17 groups are numbered. All except one group included in this study are being observed by the Germany domestic intelligence body (Bundesamt für Verfassungsschutz)³⁸ as 'suspected cases' or 'proven cases' of unconstitutional (and hence extremist) activity.³⁹

Name	Quelle
Attila Hildmann	Actively wanted by German authorities for incitement to hatred ⁴⁰
COMPACT	Verfassungsschutzbericht 2020, S. 79
Der III. Weg	Verfassungsschutzbericht 2020, S. 91
Die Kehre	Magazine published by the 'Antaios Verlag', which is being treated as a 'suspected case' of extremist activity by the Verfassungsschutz ⁴¹
Die Rechte	Verfassungsschutzbericht 2020, S. 88
Ein Prozent	Verfassungsschutzbericht 2020, S. 82
Frank Kraemer	Verfassungsschutzbericht 2019, S. 156
Gefangenenhilfe	Verfassungsschutzbericht Brandenburg 2016, S. 107
Identitäre Bewegung Deutschland	Verfassungsschutzbericht 2020, S. 108
Institut für Staatspolitik	Verfassungsschutzbericht 2020, S. 84
Kampf der Nibelungen	Verfassungsschutzbericht 2020, S. 67
Nikolai Nerling	Verfassungsschutz Lagebild Antisemitismus 2020, S. 37
Nationaldemokratische Partei Deutschlands (NPD) <ul style="list-style-type: none">- Junge Nationalisten (JN)- Deutsche Stimme (DS)	Verfassungsschutzbericht 2020, S. 86, 103, 88.
PEGIDA	Verfassungsschutz Sachsen ⁴²
PI-News	Bundesamt für Verfassungsschutz ⁴³
Sven Liebich	Verfassungsschutzbericht Sachsen-Anhalt 2019, S. 74
Uniter Network	Verfassungsschutzbericht 2020, S. 99

Endnotes

- 1 This is based on a year-over-year comparison with 2019 figures.
https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/05/pmk-2020-bundesweite-fallzahlen.pdf;session-id=D09E1BED9A5A069EB1263F917DD66198.1_cid373?__blob=publicationFile&v=3
- 2 This is based on research conducted on the monetisation platforms used by over 70 known US hate groups. Full study here:
<https://www.isdglobal.org/isd-publications/bankrolling-bigotry/>
- 3 Please see Annex 1 for the methodology and list of groups.
- 4 They are being observed as 'suspected cases' or 'proven cases' of anti-constitutional (and hence extremist) activity.
- 5 Attila Hildmann is an example of this case. It is important to note that while his sites were still live during this study, they have since been hacked and taken offline.
- 6 For examples from the US context, see: <https://www.usatoday.com/story/news/nation/2021/02/05/bitcoin-crowdfunding-used-white-supremacists-far-right-extremists/4300688001/> and <https://www.isdglobal.org/isd-publications/bankrolling-bigotry/>.
- 7 The elections will take place on 26 September 2021. See: <https://www.verfassungsschutz.de/SharedDocs/reden/DE/2021/statement-haldenwang-zur-sicherheit-der-bundestagswahl.html>.
- 8 See: <https://www.usatoday.com/story/news/nation/2021/02/05/bitcoin-crowdfunding-used-white-supremacists-far-right-extremists/4300688001/> and <https://www.justsecurity.org/74622/stopthesteal-timeline-of-social-media-and-extremist-activities-lead-ing-to-1-6-insurrection/>. Also see: <https://www.cnn.com/2021/01/13/dark-money-gop-fund-funneled-millions-groups-that-pushed-voter-fraud-claims.html>.
- 9 WooCommerce is owned and operated by WordPress. See: <https://wordpress.com/support/user-guidelines/>.
- 10 <https://www.patreon.com/de-DE/policy/community-richtlinien>.
- 11 <https://stripe.com/en-de/restricted-businesses>
- 12 <https://squareup.com/help/us/en/article/6602-understanding-square-s-terms-of-service-and-hate-prohibition-guidelines>.
- 13 <https://www.shopware.com/de/gtc/>.
- 14 <https://givewp.com/give-not-tolerate-hate/>
- 15 Der Dritter Weg is described by the domestic intelligence services as a racist and anti-Semitic organisation that is "ideologically closely aligned with the historic ideas of National-Socialism". See: <https://mdi.rlp.de/de/unsere-themen/verfassungsschutz/aufgabenfelder-und-extremismus-bereiche/rechtsextremismus/rechtsextremistische-parteien-und-parteistrukturen/>.
- 16 See: 'Give Does Not Tolerate Hate' by the CEO in October 2017 <https://givewp.com/give-not-tolerate-hate/>.
- 17 It is unclear whether these entities have charity status. Further research into this area is merited.
- 18 Banking laws in Germany require every individual to have access to a bank account. Banking services are denied in cases of risk assessment and/or illegal activity.
- 19 WooHoo Commerce is owned by WordPress. <https://wordpress.com/support/user-guidelines/>.
- 20 <https://www.paypal.com/en/webapps/mpp/ua/acceptableuse-full>.
- 21 Banking laws in Germany require everyone to have access to a bank account. Banking services are denied in cases of risk assessment and/or illegal activity.
- 22 <https://stripe.com/en-de/restricted-businesses>.
- 23 <https://newsroom.mastercard.com/news-briefs/mastercard-statement-on-the-use-of-our-network/>.
- 24 <https://www.shopware.com/de/gtc/>.
- 25 <https://www.patreon.com/de-DE/policy/community-richtlinien>.
- 26 <https://givewp.com/give-not-tolerate-hate/>.
- 27 <https://donorbox.org/acceptable-usage-policy>.

- 28 <https://www.facebook.com/communitystandards/introduction>.
- 29 <https://usa.visa.com/legal/checkout/terms-of-service.html>.
- 30 <https://www.americanexpress.com/us/legal-disclosures/website-rules-and-regulations.html>.
- 31 <https://community.dlive.tv/about/community-guidelines/>.
- 32 There are two ways in which Gambio can be used as online shop software. If the customer hosts the online shop on their own servers (own hosting), no use clauses apply to hate groups. If the software is operated via the Gambio cloud service (Gambio Cloud), the customer may not post content that is 'racist, sexist or otherwise objectionable'. See <https://www.gambio.com/legal-information/gtc-cloud>.
- 33 <https://www.westernunion.com/de/en/terms-conditions.html>.
- 34 <https://squareup.com/help/us/en/article/6602-understanding-square-s-terms-of-service-and-hate-prohibition-guidelines>.
- 35 Banks in Germany are already required to undertake anti-money laundering measures and to combat terrorist financing, among other areas of due diligence. Germany is a member of the Financial Action Task Force (FATF) standards: <https://www.fatf-gafi.org/countries/#Germany>. Also see: https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Press_Room/Publications/Brochures/2020-02-13-first-national-risk-assessment_2018-2019.html.
- 36 Banks cannot deny services to a specific political party unless they deny service to all political parties. The findings for Germany which show a reportedly high prevalence for the use of direct bank transfers are in stark contrast to a similar study conducted in the US by GDI and ISD. See: <https://www.isdglobal.org/isd-publications/bankrolling-bigotry/>.
- 37 In total, we mapped accounts on the following services (number in brackets for the whole sample): Facebook (26), Twitter (89), Instagram (13), YouTube (48), Reddit (1), TikTok (5), Vimeo (1), Spotify (1), Apple Podcasts (1), Anchor.fm (1), Breaker Audio (1), Google Podcasts (1), PCast (1), Radio Public (1), Telegram (56), Vkontakte (34), Bitchute (6), Gab (7), Parler (2), GETTR (2), Minds (0), Odysee (1), Speaker (1).
- 38 "Pursuant to section 3 (1) no. 1 case 1, section 4 (1) clause 1 lit. c, section 4 (1) clause 3 BVerfSchG, the federal and state authorities for the protection of the constitution have the mandate to collect and evaluate information on associations of persons if there are factual indications that anti-constitutional endeavours are being pursued within them. Anti-constitutional endeavours are pursued in parties or their sub-organisations if they are aimed at eliminating or invalidating the constitutional principles mentioned in section 4 (2) BVerfSchG through politically determined, goal- and purpose-oriented conduct (section 4 (1) sentence 1 lit. c BVerfSchG). If there are factual indications that anti-constitutional endeavours are being pursued in a group of persons, the Federal Office for the Protection of the Constitution, within the framework of its legal mandate, continuously observes openly perceptible activities and investigates to what extent these are of sufficient weight to establish an object of observation. The prerequisites for observation by the Federal Office for the Protection of the Constitution are met if there are sufficiently weighty factual indications of efforts by a group of persons that are directed against the free democratic basic order, i.e. are aimed at impairing or eliminating the core of the constitution." See <https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2019/fachinformation-zu-teilorganisationen-der-afd.html> [in German].
- 39 The following entities are not directly mentioned in any of the "Verfassungsschutz" reports, but still have been included due to their material and ownership linkages with other groups under observation or due to legal action against them: Attila Hildmann: Active arrest warrant by German federal protection due to hate speech and incitement to hatred; Die Kehre: This is a magazine published by the 'Antaios Verlag', which is being treated as a 'suspected case' of extremist activity.
- 40 See: <https://www.berlin.de/aktuelles/berlin/kriminalitaet/6487076-4362932-attila-hildmann-in-der-tuerkei-haftbefeh.html>.
- 41 <https://www.zeit.de/gesellschaft/2021-05/rechtsextremismus-verfassungsschutz-antaios-verlag-goetz-kubitschek-neue-rechte>.
- 42 https://www.verfassungsschutz.sachsen.de/download/2021_05_07_PEGIDA_BO_korr.pdf.
- 43 <https://www.verfassungsschutz.de/SharedDocs/reden/DE/2021/statement-haldenwang-vorstellung-des-verfassungsschutzberichts-2020.html>.
-



Beirut | Berlin | London | Paris | Washington DC

Copyright © Institute for Strategic Dialogue (2020). Institute for Strategic Dialogue (ISD) is a company limited by guarantee, registered office address PO Box 75769, London, SW1P 9ER. ISD is registered in England with company registration number 06581421 and registered charity number 1141069. All Rights Reserved.

www.isdglobal.org



The Global Disinformation Index is a UK-based not-for-profit that operates on the three principles of neutrality, independence and transparency. Our vision is a world in which we can trust what we see in the media. Our mission is to restore trust in the media by providing real-time automated risk ratings of the world's media sites through a Global Disinformation Index (GDI). The GDI is non-political. Our Advisory Panel consists of international experts in disinformation, indices and technology.

For more information, visit www.disinformationindex.org