



Middlebury Institute of
International Studies at Monterey
Center on Terrorism, Extremism, and Counterterrorism



Militant Accelerationism Coalitions:

A Case Study in Neo-Fascist Accelerationist Coalition
Building Online

Deeba Shadnia, Alex Newhouse, Matt Kriner, and Arthur Bradley
Tech Against Terrorism | Center on Terrorism, Extremism, and Counterterrorism

Executive Summary	2
Overview of Militant Accelerationism Network	4
Online Behaviours	8
Overview of findings	8
Data visualisation	10
Supporting Data	12
Methodology	15
Known entities within the network	17
Analysis of propaganda content	25
Use of Encrypted Email Services	32
Use of Website Infrastructure	34
Use of Mainstream Social Media Platforms	38

Executive Summary

Telegram has long been heavily targeted by violent far-right extremists for digital organising and community building, including for adherents to a neo-fascist strain of militant accelerationism. The so-called "Terrorgram" community¹ on the platform has been the principal point of online organising, identity building, propaganda distribution, and more.

In early 2021, two militant accelerationist coalitions emerged in the "Terrorgram" space: United Acceleration Front and National Socialist Coalition. This report provides an overview of two seemingly new formations of online networks of accelerationist and neo-fascist entities that are self-described as Atomwaffen Division (AWD) spinoffs. It also provides an understanding of how they behave online and speaks to the threats of real-world violence they pose.

One such inspired entity is Feuerkrieg Division (FKD), which is at the centre of the two networks assessed in this report. FKD, which is a proscribed entity in the UK, Australia, and Canada, emerged in early 2021 from a period of dormancy in order to promote and network with InJekt Division. InJekt and FKD provided established networks and aesthetic machinery to help build the United Acceleration Front and National Socialist Coalition.

CTEC and Tech Against Terrorism collected and analyzed data from channels and chats associated with these coalitions from June 2021 to February 2022. Having archived consistently throughout that period, this data provides an unprecedented snapshot of the evolution of neo-fascist coalition-building and the ways that extremist actors strategically use communications (and sometimes expunge past messages) for propaganda purposes on Telegram.

We augmented this primary data with context beyond this timeline. Throughout this report, we show that these coalitions are consequences of a pattern of activity that emerged years before.

Tech Against Terrorism identified 21 entities within this network over the period of June 2021 to February 2022. The network was densely populated by distinct but seemingly allied entities. A key feature of the network's operation was the announcement of strategic partnerships between entities. Based on our analysis of domain records relating to websites run by entities within the network, we assess it to be likely that the apparent strength of this network may have been artificially inflated by its creators, who likely sought to make the network appear larger than it was.

Typical behaviours observed across the network include:

- Using Telegram to announce the creation of named entities, to recruit members, and to disseminate propaganda externally.
- Supplementing the network's core presence on Telegram with accounts and pages in other online spaces, including mainstream social media platforms.

¹ The name "Terrorgram" is a combination of Telegram and terrorism. Members of neo-fascist Telegram channels overtly endorse militant accelerationism, terrorism, and excessive racism and anti-Semitism.

- The explicit amplification of allied entities within the network. Telegram channels would regularly promote other channels and groups with shared ideologies and goals, through resharing of posts, sharing of relevant URLs, and encouraging users to subscribe to their partners' channels or pages.

Overview of Militant Accelerationism Network

Neo-fascist accelerationists—and militant accelerationists writ large—maintain a loose constellation of cells and groups, which operate as a network that embraces a branding strategy of "continual collapse, reshuffling, and reemergence."² Entities such as AWD serve less as a central command or an umbrella structure and more as a brand that can be adopted and dropped at will by sympathetic or aspiring cells that lack meaningful structural links. This strategic approach presents analysts, practitioners, and law enforcement agencies with significant challenges in determining the authenticity of, and risks posed by, emergent factions within accelerationist organising online.³



Figure 1: Image created by Iron March users.

Inspired by historical terrorist movements, this strategy emerged from the Iron March forum, the defunct incubator for militant accelerationists. Operational from 2011-2017, the forum served as a town square for neo-fascists, facilitating the development of a group of militant neo-fascist entities that became the backbone of the contemporary transnational accelerationist network commonly referred to as the "skull mask" network.⁴ As Alex Newhouse wrote:

² Alex Newhouse, "The Threat Is the Network: The Multi-Node Structure of Neo-Fascist Accelerationism," CTC Sentinel 14:5 (2021), <https://ctc.usma.edu/the-threat-is-the-network-the-multi-node-structure-of-neo-fascist-accelerationism/>

³ Jon Lewis and Alex Newhouse, "Be Careful Attributing Anything to AWD", *The Accelerationism Research Consortium*, (n.d.), <https://www.accelresearch.org/shortanalysis/be-careful-attributing-anything-to-awd>

⁴ H.E. Upchurch, "The Iron March Forum and the Evolution of the "Skull Mask" Neo-Fascist Network, CTC Sentinel 14:10 (2021), <https://ctc.usma.edu/the-iron-march-forum-and-the-evolution-of-the-skull-mask-neo-fascist-network/>

"At its height, the website and the network it had facilitated allowed extremist and terrorist groups to outsource certain important infrastructural and developmental tasks to the crowd, such as the creation of propaganda materials and collaboration on organizational development.⁵ Users also shared tactical guidebooks alongside ideological and philosophical material, ranging from bomb-making manuals to Nazi tracts and occult books.⁶"

Creators from the Iron March forum themselves provided explanations for the iconography within the Iron March crest, which further informs our understanding of how later networks formed. The top right quadrant's three wolfsangel symbols is meant to signify the "network of websites and online projects created by the IronMarch community and its individual members."

At the crest's centre is the "skull mask" which is meant to signify "the face of 21st Century Fascism, rejection of individualism and egoism - we follow and serve the Truth."

Iron March users also created new groups, such as AWD, which popularised the skull mask, and engaged in offline training and activity together. Ultimately, the skull mask network explicitly advocates "for the violent overthrow of governments and the creation of totalitarian Aryan nations."⁷ As H.E. Upchurch detailed in "The Iron March Forum and the Evolution of the 'Skull Mask' Neo-Fascist Network":

"The history of the Iron March network shows that violent extremist movements can develop from online communities even in the absence of a territorial base and without regular in-person contact between members. Iron March provided a closed social space where young neo-fascists who did not fit in well in established neo-fascist organizations could create a transnational collective identity."⁸

Legacy groups like AWD have inspired additional organising and offline activity that draws heavily from the Iron March aesthetic and tactics. The recent Telegram-based networks, United Acceleration Front and National Socialist Coalition, make aesthetic, branding, and structural decisions which indicate a high likelihood of deep familiarity with Iron March and an attempt to leverage its legacy.

⁵ James Poulter, "The Obscure Neo-Nazi Forum Linked to a Wave of Terror," Vice News, 12 March 2018, <https://www.vice.com/en/article/437pkd/the-obscure-neo-nazi-forum-linked-to-a-wave-of-terror>.

⁶ Alex Newhouse, "The Threat Is the Network: The Multi-Node Structure of Neo-Fascist Accelerationism," CTC Sentinel 14:5 (2021), <https://ctc.usma.edu/the-threat-is-the-network-the-multi-node-structure-of-neo-fascist-accelerationism/>

⁷ *Ibid.*

⁸ H.E. Upchurch, "The Iron March Forum and the Evolution of the "Skull Mask" Neo-Fascist Network, CTC Sentinel 14:10 (2021), <https://ctc.usma.edu/the-iron-march-forum-and-the-evolution-of-the-skull-mask-neo-fascist-network/>



Figure 2: Iron March groups affiliations image created by users (top left) and National Socialist Coalition (top right) and United Accelerationist Front (bottom centre) versions of their network affiliations.

These two networks were aesthetically positioned to evoke Iron March-era organising. Telegram channel profile images for the networks further illustrate the aesthetic inheritance by the two networks and their constituent groups. Strong parallels include the widespread use of variations on the SS Division shield logo [above], a practice begun by AWD and the Iron March network, as well as pattern and shape similarities in the banner logos [below].



Figure 3: Three example banner logos in the Iron March format (left). The additional two are National Socialist Coalition (centre), and Waldjäger group (right).

Notably, both networks likely formed entirely online and were connected by FKD, a "Siegist" group that was created in 2018 and quickly expanded across Europe and North America. FKD emerged in the second main wave of Siegist groups,⁹ promoted "Universal Order" ideals popularised by James Mason and Charles Manson, and shared members with AWD, The Base, and other groups.¹⁰ After going dormant during 2020, FKD re-emerged with a new co-leader in order to promote the activities of InJekt Division. That co-leader uses various pseudonyms, but for the purposes of this report will be referred to as Hergle Zelea. Critically, Hergle Zelea used the FKD platform to establish himself as a central figure in the Terrorgram community, and he served as a core organiser in the development of UAF and National Socialist Alliance.

⁹ The first wave was composed of Iron March-era groups, including AWD, Antipodean Resistance, and National Action.

¹⁰ <https://ctc.usma.edu/the-threat-is-the-network-the-multi-node-structure-of-neo-fascist-accelerationism/>

Online Behaviours

Overview of findings

Introduction

This section outlines the online behaviours of a network of neo-fascist accelerationist actors, including FKD and InJekt Division, some of which directly claim to be "spin-offs" of terrorist group AWD and its affiliates. Tech Against Terrorism identified 21 entities within this network over June 2021 - February 2022. At the time of writing, at least ten of these entities appeared to still be active online.

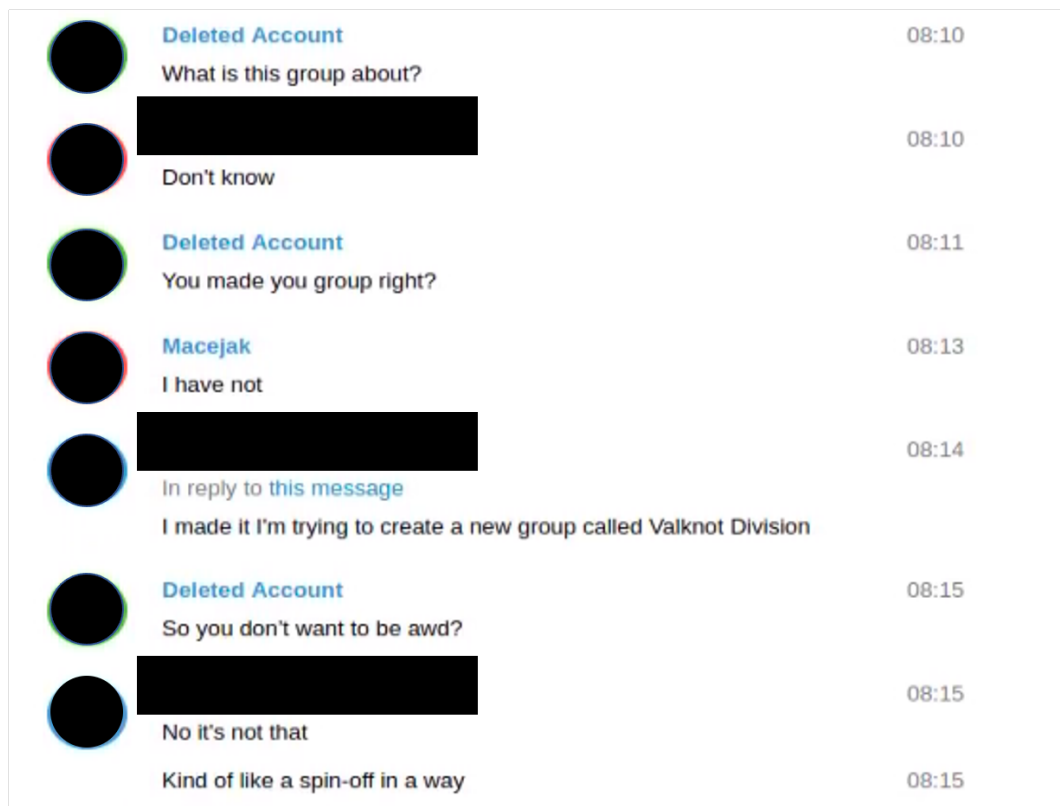


Figure 4. Screenshot taken of a Telegram chat linked to a channel named Valknot Division, where the admin of the channel refers to the entity being a "spin-off" of AWD. Tech Against Terrorism acknowledges that it is unlikely Valknot Division had operational ties to AWD, but was more likely referring to the wider AWD 'brand' that has been established following the disruption of AWD in 2019.¹¹

¹¹ Jon Lewis and Alex Newhouse, "Be Careful Attributing Anything to AWD", *The Accelerationism Research Consortium*, (n.d.), <https://www.accelresearch.org/shortanalysis/be-careful-attributing-anything-to-awd>

Origins of network

We first identified this online network in June 2021, which largely originated on Telegram. The vast majority of these entities had a short online life-span due to channel suspensions by Telegram's moderators, and did not resurface online after being deplatformed. The most notable features of how this network behaved during the data collection period are:

- The network was densely populated by distinct but seemingly allied entities. Announcements of strategic partnerships between multiple entities within the network was a key feature of how the network was operating. At the time of writing, the network was largely dormant due to several factors, including consistent content moderation efforts by Telegram.
- The groups within this network were frequently suspended by Telegram and whilst a small proportion would persistently reappear, many would often not attempt to return once they had been deplatformed.
- There was frequent infighting amongst members and admins of these channels on Telegram.
- At least three coalitions arose over the monitoring period that sought to establish unified relationships and amplify the entities within the network to as wide an audience as possible.

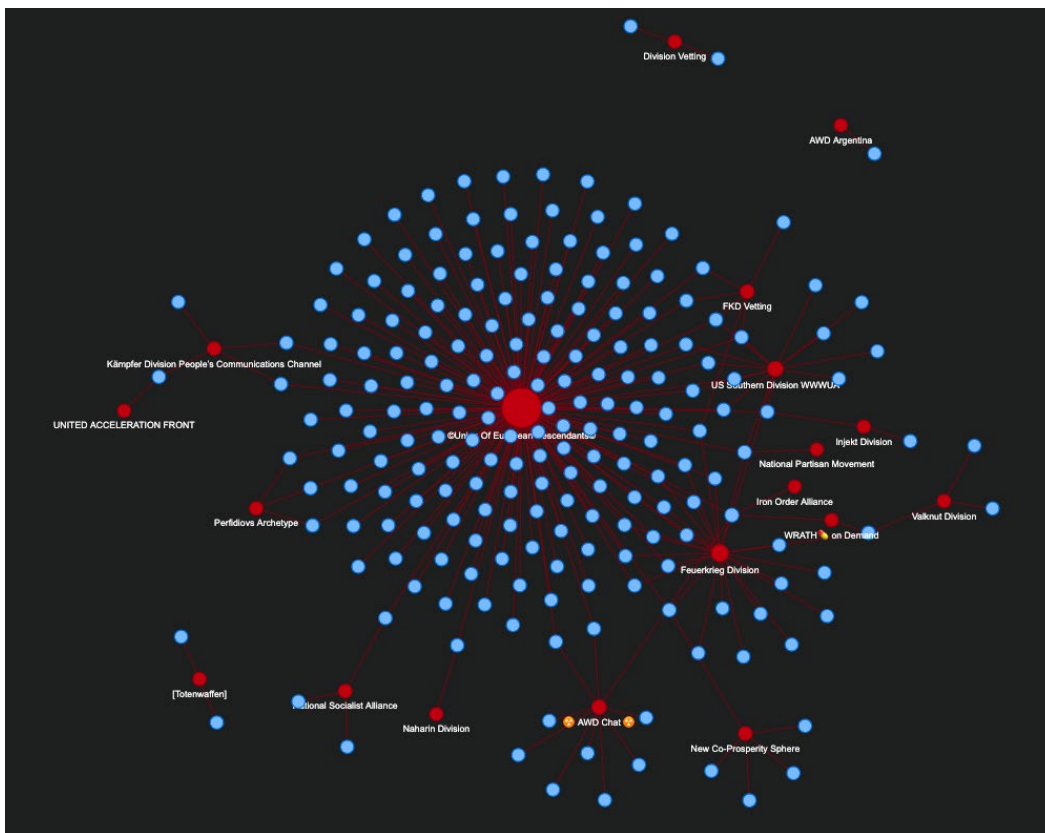
Data visualisation

The data visualised below emphasises the networked nature of the neo-facist accelerationist online landscape. The results are based on Tech Against Terrorism's proactive monitoring of how these entities behaved online between June 2021 to February 2022. The data consists of Telegram chat downloads that were accessible at the time of research. Some of these channels, groups and private chats have since been de-platformed, while others remained active online at the time of writing.

Our methodology of data collection was near daily downloads of Telegram channels, groups and chats that our team came across during monitoring. An entity was included in the dataset if it had interacted with or been promoted by an already established node in the neo-facist accelerationist online network.

The data below is not fully comprehensive, as our archive contained gaps due to lack of access to certain private groups, frequent takedowns by Telegram, and the shifting nature of the wider violent accelerationist landscape on the platform.

Some notable entities within the network that have significantly impacted the outcome of the data include the highly active neofascist propaganda channel and its affiliated chat - WWWUA and Union of European Descendants - that actively seek to unify several otherwise disparate communities across Telegram.



Inauthentic amplification

Tech Against Terrorism assesses that the apparent strength of this neo-facist accelerationist network may be artificially inflated by its creators, who seek to make the network appear larger than it is. This is based on evidence that a handful of administrators managed multiple channels within this network simultaneously. This report explores this evidence further on page 35. Furthermore, domain records show that several websites linked to this network were at one time hosted on the same IP address. This suggests these sites were likely to be managed by a single entity.

The likely superficial exaggeration of this network by its creators should not diminish the real world threat that members of this network potentially pose. In June 2021, officials in Texas thwarted a plot to attack a Walmart by an active member and suspected cofounder of one of the groups in this network, InJekt Division.¹²

There are strategic benefits for terrorist and violent extremist actors to operate within diffused networks such as the one covered in this report. Primarily, actors within a network can often use their connections to grow their own audience base and membership. This was particularly the case given active attempts by the channels in the network at encouraging subscribers to follow/subscribe or otherwise follow their allies. Furthermore, a networked structure of operation ensures that if one entity is removed, the network remains on the whole intact.

¹² Mack Lamoureux, "Neo-Nazi was behind Walmart Mass Shooting plot, group claims", *Vice News*, 31 May 2021, <https://www.vice.com/en/article/z3xmnw/neo-nazi-was-behind-walmart-mass-shooting-plot-group-claims>

Supporting Data

Key behaviours

Through daily monitoring, our team identified that the network was broad, with some nodes being more integral and active to the wider structures of movement than others. For example, a Telegram channel named Feuerkrieg Division (FKD) is a notable group in this network, as it has been extremely active on Telegram. It is unclear whether this online entity is directly operationally linked with the FKD group that was established in 2018.¹³

It is possible that this new iteration has co-opted the FKD "brand", though for the purposes of this report, our team will treat this entity as a legitimate FKD online account. Between June 2021 - February 2022, TAT identified eight separate FKD channels that were active across this network. At the time of writing in February 2022, FKD operated one account and channel on Telegram.

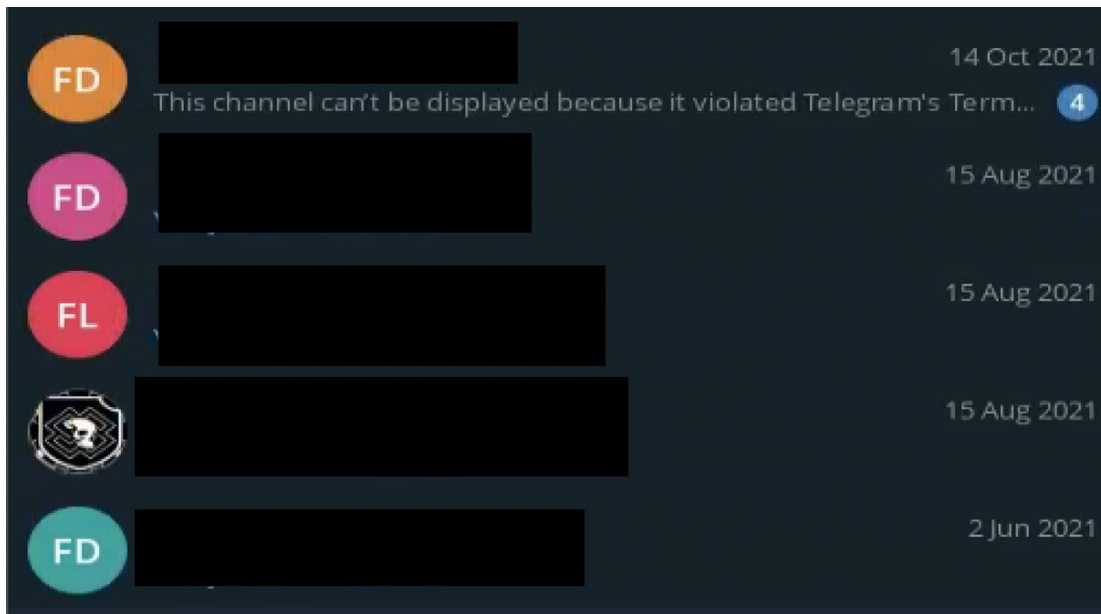


Figure 5. Examples of the different iterations of FKD channels/groups and private chats that were active over the monitoring period.

Telegram routinely banned FKD channels during the data collection period, however the group repeatedly returned to the platform with the same name and logo in order to conduct its activities. These are namely the dissemination of propaganda, recruitment and internal communication.

Similar to FKD, InJekt Division served as a central figure in the network throughout the data collection period since we first identified it. Our team identified at least five Telegram channels, groups and private chats related to the group. In June 2021, InJekt Division announced an "alliance" with FKD, and actively

¹³ "Feuerkrieg Division", *Anti-Defamation League*, n.d., <https://www.adl.org/resources/backgrounders/feuerkrieg-division-fkd>.

promoted the FKD Telegram channel to its subscribers. A private InJekt Division channel remained active at the time of writing.

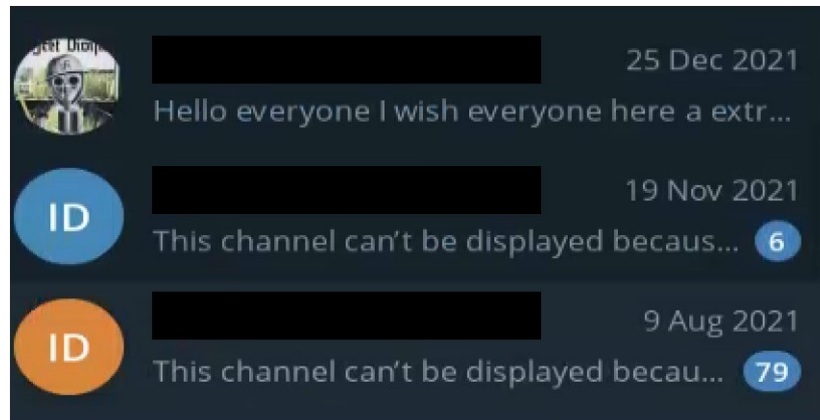


Figure 6. Screenshot depicting three separate InJekt Division Telegram channels that were active between August - December 2021. All had been suspended by Telegram's content moderators.

The entities within this wider neo-fascist online network all exploit online spaces in very similar ways. Most entities first establish their online presence on Telegram, before then directing users to other online spaces such as websites or encrypted email services. Following this, usually in a matter of days or weeks, the entities were either deplatformed, deleted themselves, or simply ceased their online activities.

The most typical behaviours across the network included:

- Using Telegram as a "beacon" platform to first announce their creation, as well as to disseminate propaganda externally and recruit members.
- Supplementing their core Telegram presence with accounts on other online spaces, including mainstream social media platforms.
- Establishing their own websites that archive propaganda content and allow for online users to get in contact with website admins.
- Explicit amplification of allied entities within the network. This takes the form of Telegram channels promoting other channels and groups with shared ideologies/goals, through re-sharing of posts, sharing of relevant URLs, and encouraging users to subscribe to their partners.

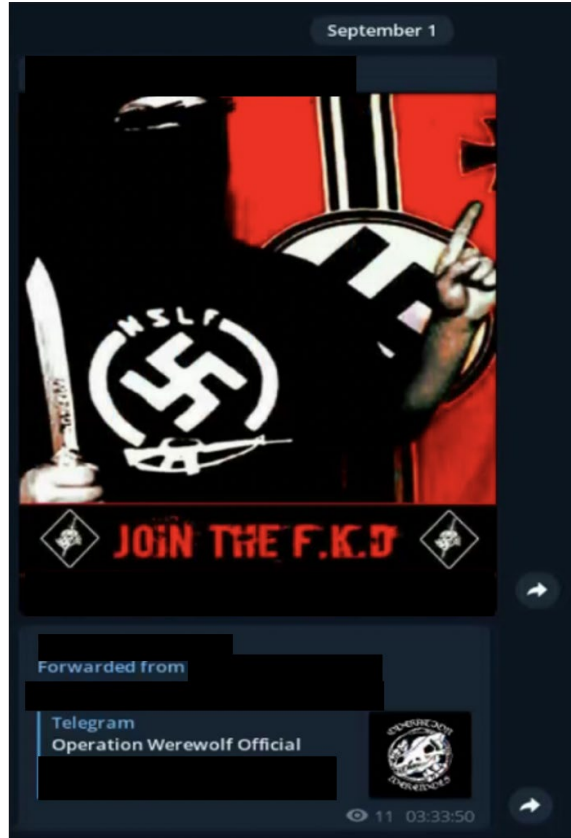


Figure 7. Screenshot highlighting the nature of the networked aspect of how these online actors operate. The post depicts a FKD channel promoting a post by InJekt Division, that was in turn promoting a channel named "Operation Werewolf". Affiliation between entities was depicted through the forward function on Telegram, and the intended and curated amplification of one another's content/channels.

Methodology

Our findings cover the period of June 2021 - February 2022, as we monitored this network across a variety of mainstream and niche online spaces. Our monitoring consisted of daily OSINT tracking of publicly accessible channels, groups and chats on Telegram, as well as other platforms such as Wire, Twitter, Instagram, and static websites.

All OSINT monitoring was conducted using sockpuppet accounts. Our teams did not engage with any entity or individual, nor did we pose as a terrorist or violent extremist actor. In some instances, our team gained access to private group Telegram chats after admins posted joinlinks to publicly accessible channels. Any channel or group that required verification, vetting or further engagement or interaction was not accessed.

Our monitoring used a combination of the following techniques to track the neo-facist accelerationist online network:

- Daily English language keyword searches in Telegram relating to known entities within the network to identify newly created channels or groups. Our team limited searches to English, the primary language used by members of the network.
- Daily downloads of Chat Data using Telegram's in-app export function.
- Keyword searches using advanced search queries on search engines such as Google and Bing for associated accounts and websites elsewhere online.
- As Telegram was the primary location of this network's activities, we conducted daily monitoring of relevant chats in order to identify additional URLs leading to other online spaces, such as websites or other messaging platforms.
- Monitoring of dark web spaces to identify the extent to which this network was seeking to establish archives or backups on the dark web. We did not identify evidence that the network was exploiting the dark web in any coordinated manner.

We acknowledge the limitations to our research, namely:

- Due to our non-engagement with terrorist and violent extremist actors, our understanding of how these entities behave stops at the point where contact is necessary for further investigation.
- While all the entities within this network communicate primarily in English, limiting relevant keyword searches to English may have restricted our ability to assess how these networks interact with transnational actors across multiple languages.¹⁴

Our justification for including an entity as being within this network relied on at least one of the following factors:

- Any entity that was directly promoted by another group in the network, either in the form of propaganda, or posting URLs relevant to the entity. For example, FKD promoted content from the Totenwaffen channel proclaiming their involvement in the Iron Order, warranted inclusion of Totenwaffen within the network.

¹⁴ Further investigation is needed to assess the extent to which this network interacts with other global neo-facist accelerationist actors.

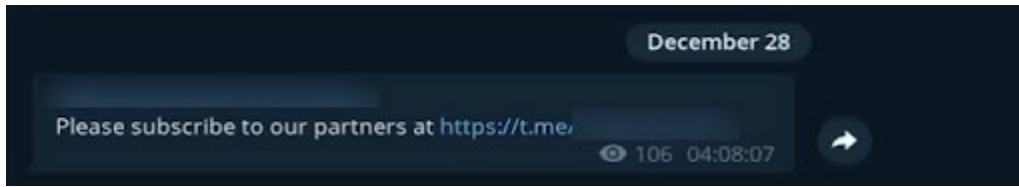


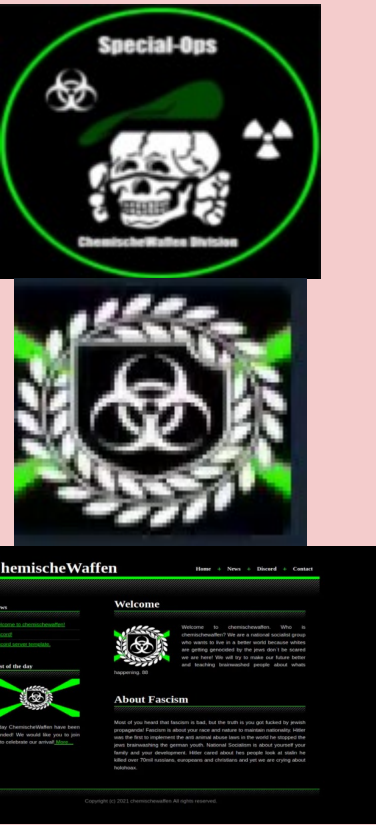
Figure 8. Another example highlighting how nodes within the network would actively amplify one another by urging subscribers to joining other channels and groups.

- Any entity that has been named in the broader coalitions or groups that sought to formalise the relationships between entities. Examples include any entity named within the Iron Order, National Socialist Coalition or the United Acceleration Front.






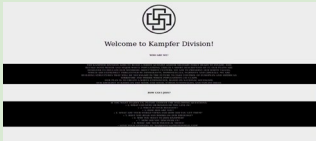

Known entities within the network



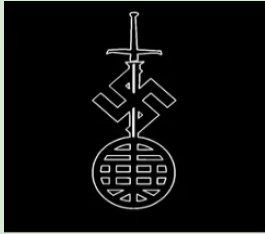



- Inactive at the time of writing - There is no known active or dormant associated channel or group on Telegram or elsewhere online
- Active at the time of writing - There is either an active or dormant associated channel or group on Telegram, or active elsewhere online

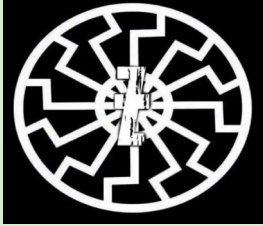
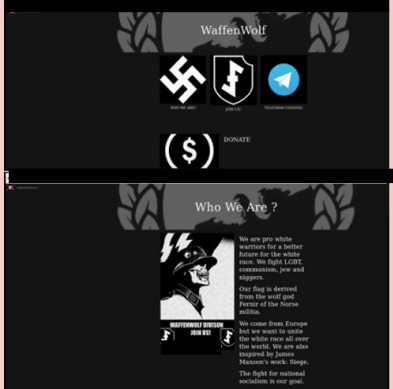


Due to the unavailability of some data at the time of writing, the below table does not present a conclusive list of all known entities and their associated logos or URLs within the accelerationist neo-fascist online network.¹⁵

	Name	Logos/ Relevant images
1.	Atomwaffen Division Argentina	
2.	Chemische Waffen	 <p>The image shows three distinct visual elements related to the 'Chemische Waffen' entity. At the top is a circular logo with a black background and a green border. It features the text 'Special-Ops' at the top, a biohazard symbol on the left, a skull in the center, and a radiation symbol on the right. Below the skull, the text 'ChemischeWaffen Division' is visible. Below this is a square logo with a black background and a green border, featuring a white biohazard symbol centered within a laurel wreath. At the bottom is a screenshot of a website titled 'ChemischeWaffen'. The website has a black background with green text and accents. It includes a navigation bar with 'Home', 'News', 'Divided', and 'Contact'. The main content area has a 'Welcome' section with a biohazard icon and an 'About Fascism' section. A footer at the bottom reads 'Copyright © 2021 chemischewaffen. All rights reserved.'</p>

¹⁵ Data is unavailable either due to channels, websites and other online spaces being de-platformed before CTEC and TAT were able to download the historic data, and/or a lack of access to the data via the Internet Archive and other open-source databases.

3.	<p style="text-align: center;">Feuerkrieg Division</p>	
4.	<p style="text-align: center;">InJekt Division</p>	
5.	<p style="text-align: center;">International White Syndicate</p>	
6.	<p style="text-align: center;">Kampfhund</p>	
7.	<p style="text-align: center;">Kämpfer Division</p>	 
8.	<p style="text-align: center;">Kriegswaffen Division</p>	




8.	<p style="text-align: center;">Naharin Division</p>	
9.	<p style="text-align: center;">Nationalist Partisan Movement</p>	
10.	<p style="text-align: center;">New Co-Prosperity Sphere (NCPS)</p>	
11.	<p style="text-align: center;">Reinstes Division</p>	
12.	<p style="text-align: center;">Sturmjager</p>	
13.	<p style="text-align: center;">Totenwaffen</p>	<p style="text-align: center;">TOTENWAFFEN</p> 

14.	Totennacht Division	
15.	Valknut/Valknot Division	
16.	Waffen Wolf Division	
17.	Waldjäger Division	
18.	X Network (Cult 88)	

Coalitions within the network

One central feature of this network's online behaviour was the establishment of several "coalitions" that sought to tie entities together in a formalised way. These coalitions acted as aggregators of neo-fascist content on Telegram, and sought to amplify individual groups within each coalition to as wide an audience

as possible. It is highly likely that at least three of these entities were administered by a single individual or group, based on our research.

19.	<p style="text-align: center;">Iron Order Alliance</p>	
20.	<p style="text-align: center;">Nationalist Socialist Alliance</p>	
21.	<p style="text-align: center;">United Acceleration Front</p>	

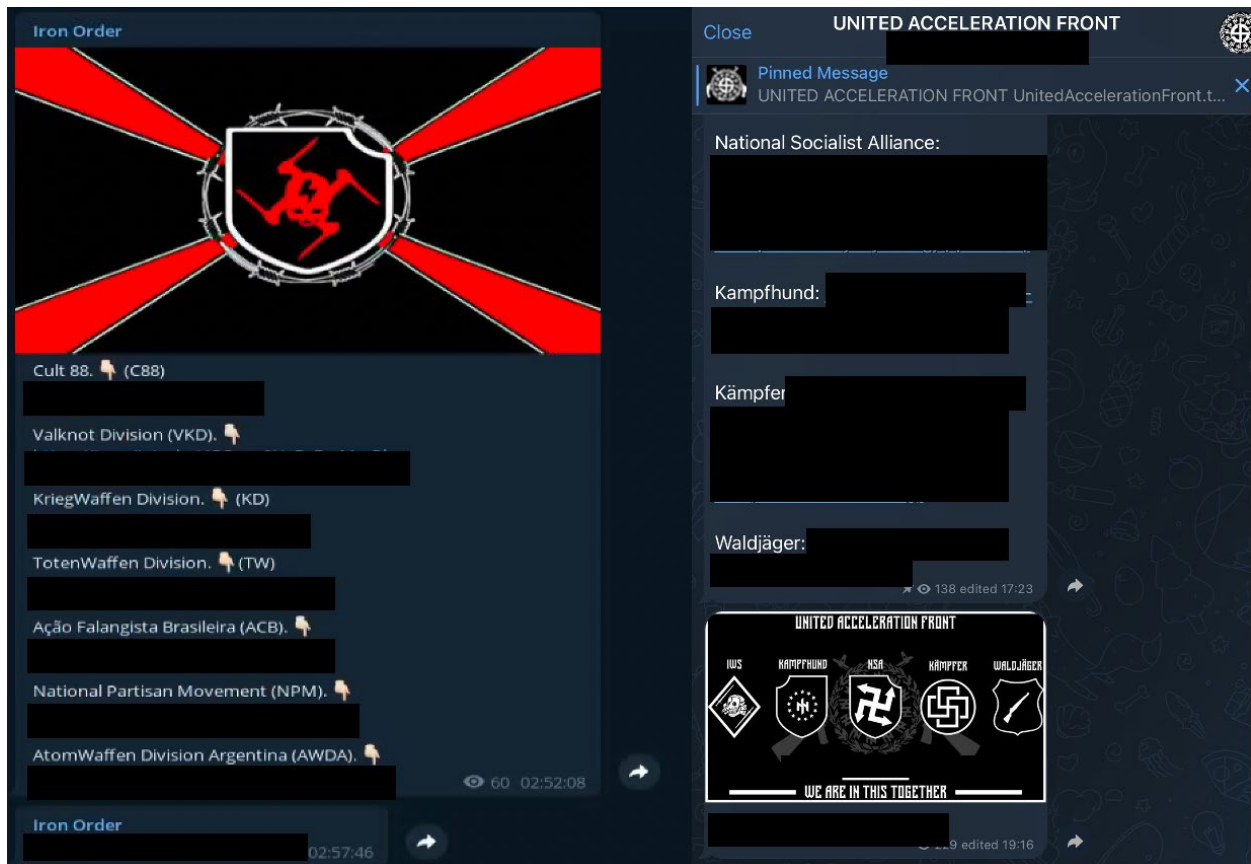


Figure 9. Screenshots of Iron Order (left) and United Acceleration Front (right) on Telegram. These entities sought to build coalitions and official partnerships



Figure 10. Screenshot taken of propaganda material disseminated by the United Acceleration Front Telegram channel. Listed in this poster is the International White Syndicate, Kampfhund, National Socialist Alliance, Kämpfer Division, Waldjäger Division.

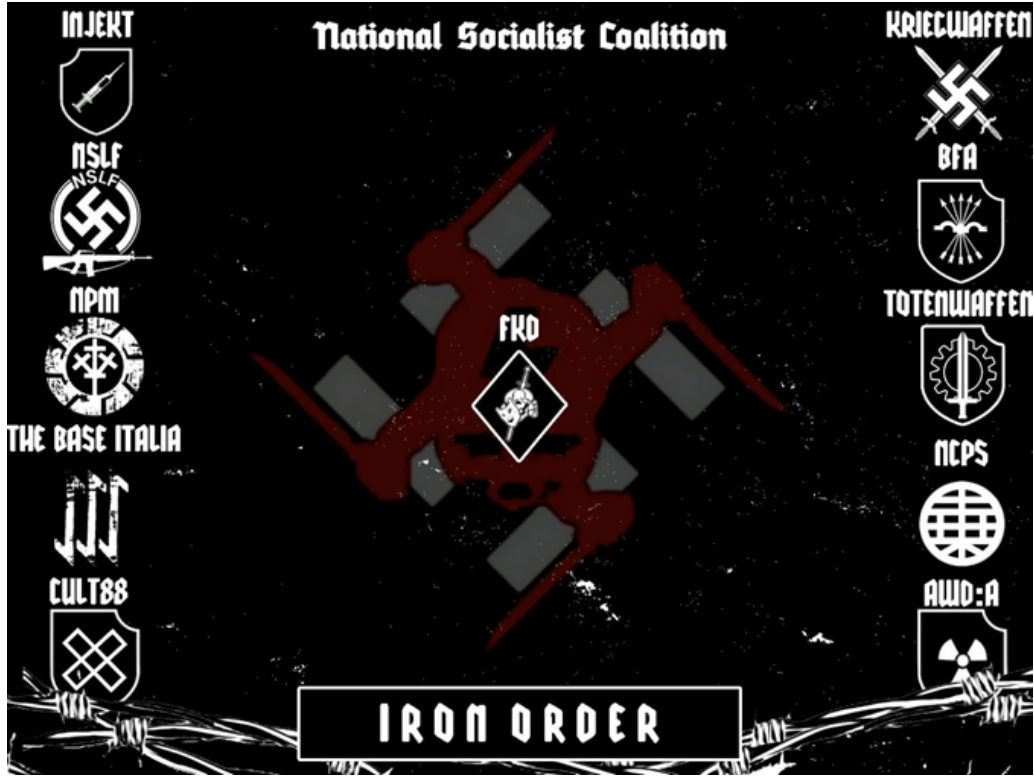


Figure 11. Screenshot taken from propaganda content that was disseminated by the Iron Order Telegram channel. In this poster the following entities are listed, from top-left: InJekt Division, National Socialist Liberation Front (NSLF), National Partisan Movement (NPM), The Base Italia, Reinstes Division, Kriegwaffen Division, BFA, Totenwaffen Division, New Co-Prosperity Sphere, Atomwaffen Division Argentina.



Figure 12: Image of network affiliates for Iron March created by users of Iron March. In this poster the following entities are listed as "affiliated groups", from top-left: National Action, Skydas, Atomwaffen Division, Antipodean Resistance. The following entities are listed as "supported groups," from top-right: Nordic Resistance Movement, Golden Dawn, Casa pound, Serbian Action, Azov.

Analysis of propaganda content

The entities within this network disseminated stylistically similar propaganda material, which mainly took the form of promotional posters and diagrams. Images and rhetoric heavily overlapped with Iron March and "Siegest" aesthetics. In fact, *none* of the items shared by UAF or National Socialist Alliance appear to be new, suggesting that they were recycling AWD and Iron March content. This is a strong indication that these networks were attempting to leverage the AWD / Iron March branding and shared visual language in accordance with that branding, as opposed to forging a new direction for the accelerationist movement.

Additionally, we identified numerous propaganda items originally created by Patrick MacDonald, an artist better known by the moniker "Dark Foreigner."¹⁶ Although he only became active during 2017, the last year of Iron March's operations, Dark Foreigner's recognizable, digestible, and striking style established him as the go-to propagandist for the *siegekultur* aesthetic emerging at that time. He became the de facto chief propagandist for the entire skull mask network, including AWD, FKD, and Sonnenkrieg Division. UAF and National Socialist Alliance's repackaging of Dark Foreigner-created and -inspired imagery is testament to MacDonald's lasting legacy within the movement.

Much of the propaganda content shared by the network explicitly endorsed and promoted violence. Some content openly encouraged supporters to engage in acts that, it claimed, would hasten the collapse of society and bring about total civilizational collapse. An image posted in the National Socialist Alliance in December 2021 illustrates this strategic approach and desired outcome. The post was shared from "The American Futurist Official" channel, which is a Telegram channel affiliated with the website that is run by the National Socialist Order (NSO).

¹⁶ Ben Makuch and Mack Lamoureux, "Unmasking 'Dark Foreigner': The Artist who fueled a neo-Nazi terror movement", *Vice News*, 7 July 2021, <https://www.vice.com/en/article/93ynv8/unmasking-dark-foreigner-the-artist-who-fuelled-a-neo-nazi-terror-movement>.



Figure 13: Telegram screenshot illustrating the strategic approach to societal collapse endemic to the neofascist accelerationism community.

Significantly, all propaganda posted by UAF or National Socialist Alliance channels themselves (i.e., not forwarded) was branded with the individual group's logo or phrase, and nearly all content included information for how to contact the group's admins elsewhere online. This was likely in order to both encourage Telegram users to engage with channel admins off the app, as well as for the posters to be distributed to other online spaces outside of Telegram so as to ensure their email addresses were the primary source of internal communications. Monitoring did not identify a significant volume of original propaganda video content across the network.

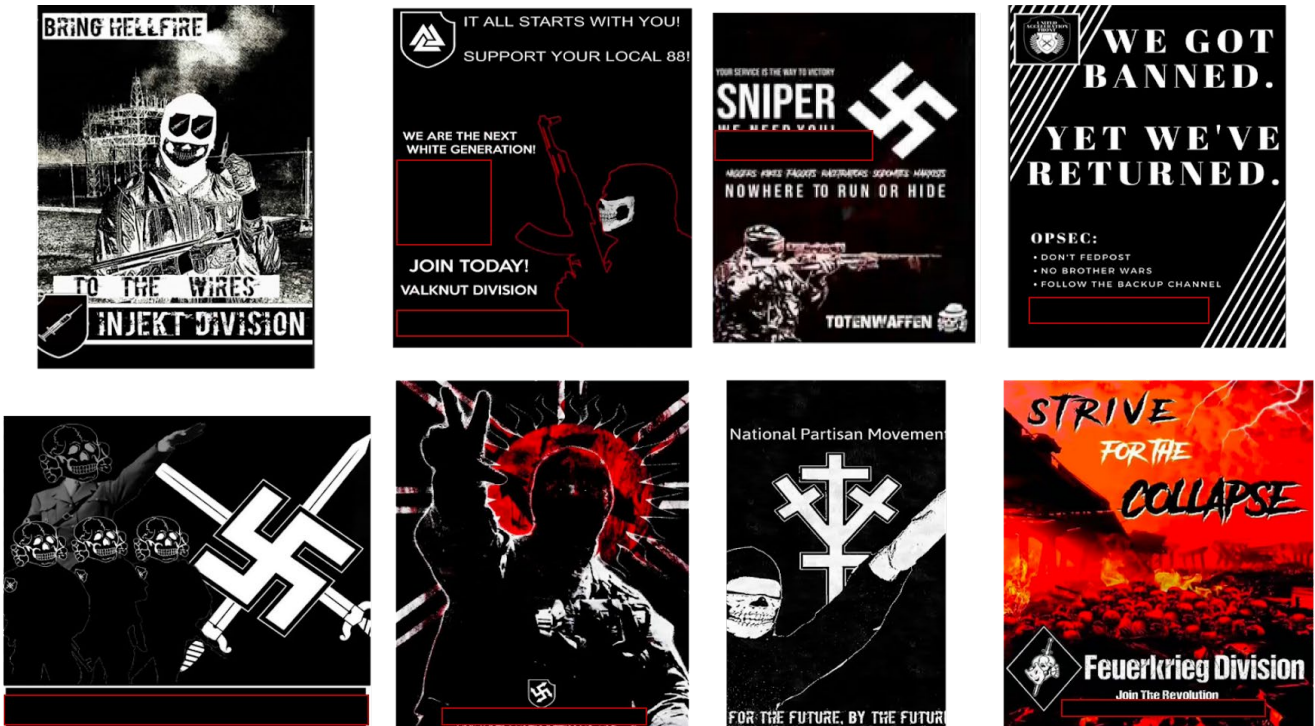


Figure 14. Collection of screenshots of propaganda posters disseminated by entities within the online network. In all cases, screenshots were taken from Telegram channels or groups. Nearly all propaganda material incited violence or sought to promote the neo-fascist accelerationist ideology. Furthermore, in most cases, posters included contact details for E2EE email addresses.

Ideological Influences

Siege

Content within the channels often followed the aesthetics established by Dark Foreigner and the skull mask network in 2017-2018. Referred to variously as "Siegism," "Siege Culture," or "Siegekultur," this aesthetic trend is based on a shared admiration for Charles Manson, William Luther Pierce, and, especially, James Mason. James Mason's *Siege* provided most of the tactical, strategic, and rhetorical basis for the operations of the skull mask network, and Mason himself assumed an active role in AWD and, later, NSO.

Siege stresses the use of small-cell, decentralised, geographically-dispersed violence in order to have a disproportionately chaotic impact on the day-to-day operations of society. The central argument is that a very small number of dedicated neo-fascist terrorists have the ability to spark a race war, revolutionary upheaval, and civilizational collapse without putting together an entire army or mass uprising. With help from Mason himself, the skull mask network developed shared aesthetics and rhetoric designed to evoke the ideas of *Siege*.

The National Socialist Alliance and United Acceleration Front frequently employed the markers of Siege Culture. "Siegefont," a spiky, aggressive-looking typeface first developed for AWD posters, is found throughout propaganda published in these channels. Imagery promoting wholesale apocalyptic destruction and glorifying terrorists further strengthen the connection to Siegism.

Christian Identity

Across various channels, we detected influences reminiscent of Christian Identity in posts and propaganda created and shared. The National Partisan Movement (NPM) channel posted multiple overt references to Christianity, an abnormal pattern in a digital community that often idolises Norse paganism and is frequently outright hostile to the Christian faith. NPM's logo, a combination of four Christian crosses in the shape of a Tyr rune, is another example of an unusual fusion of neo-pagan and Traditionalist iconography with symbols of Christian faith.

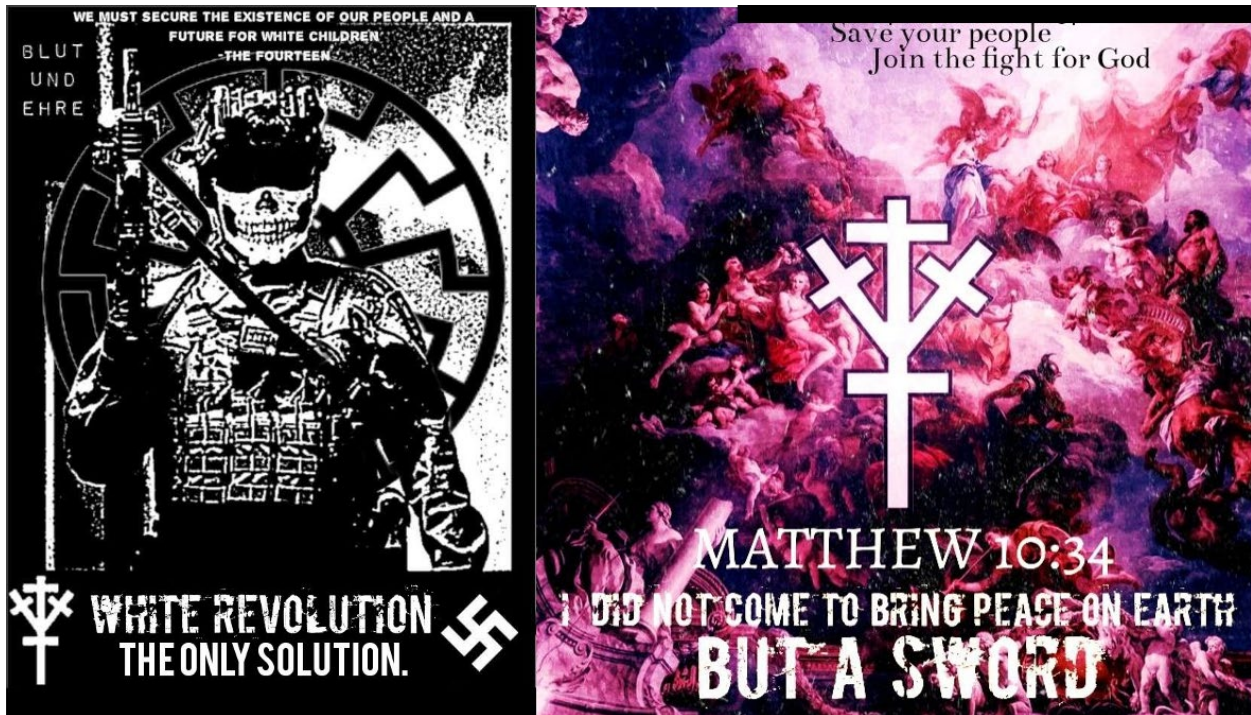


Figure 14: Telegram screenshots of propaganda posters disseminated by National Partisan Movement that indicate use of Christian Identity and Christianity themes.

The posts above directly invokes the 14 words, a white supremacist slogan, and mixes the concept with a Bible Verse. This is standard practice for Christian Identity adherents. However, we assess the use of Christianity in these posts to likely be an intentional recruitment effort as opposed to an expression of a sincerely held religious belief.

The below image was also shared by the NPM. It clearly depicts the skull mask above two books, one of which is the Christian Bible and another which is obscured. The post is similar in structure to staged images shared by satanist Order of Nine Angles (O9A) adherents who will engage in a practice known as "Insight roles." During an Insight role, an O9A initiate will undertake an infiltration of another extremist group with the goal of making it more receptive to O9A teachings or, barring that, simply more primed for accelerationist violence. Insight roles are also used for furthering the initiatic education of O9A recruits, giving them deep understanding of the milieu in which they immerse themselves.



Figure 15: Image uploaded to the National Partisan Movement Telegram channel displaying a skullmask, Christian Bible, and National Partisan Movement branded division shield reminiscent of Order of Nine Angles shrines.

This activity matches trends identified by CTEC related to an increase of Christian Identity ideology across the broader accelerationist landscape. First, in data reviewed beyond this report's scope, CTEC has identified a defined uptick of likely infiltrations (or insight roles) by O9A adherents into the broader Christian Identity movement online. Second, CTEC has detected a considerable increase in Christian Identity influences on propaganda in various sub-milieus of the accelerationist movement, such as Boogaloo, militias, neo-Nazis, among others.

These two trends are not mutually exclusive as infiltrations are often defined by the introduction of militant accelerationist or militant Traditionalism content into existing social media communities. We assess these trends to be an exemplar of militant accelerationists' goals of pushing already radicalised communities into active violence to destabilise the system, as well as to move millenarian oriented ideologies towards militant Traditionalist views exemplified by overt militant accelerationists such as AWD, the Base, and O9A.

Use of Telegram as a "beacon" platform

All actors within this network sought to exploit encrypted messaging platforms - specifically, Telegram, and to a lesser extent, Wire - for a wide array of operational and strategic objectives. Much like violent Islamist use of encrypted messaging platforms, neo-fascist accelerationist actors in this network used Telegram as a "beacon" platform, where they would first disseminate content on these channels and then direct users elsewhere online. Beacon platforms can also facilitate communication between members and supporters of a group, as was the case for the National Partisan Movement, whose channel allowed for users to communicate directly with admins.¹⁷

All groups within the network used Telegram in similar ways. Groups would first announce their creation on Telegram in a public channel. In some cases, channels would later create private groups which were accessible via invite link only. These invite links would often be posted in public channels, so as to increase the membership size of the groups.

Consistent de-platforming

Widespread and frequent deplatforming of channels by Telegram played a key role in how this network behaved. As a result of consistent content moderation, the majority of the entities within the network had a short life-span of no more than a few days or weeks. Significantly, at the time of writing, very few of the entities in the network had retained their original channel or group on Telegram.

Despite frequent removals, some entities would return often hours or days later, usually with a variation of their name that allowed them to still be recognizable (like Totenwaffen 2). Although replacement accounts were also often banned by Telegram, this highlights the risk Telegram and other platforms face with terrorist and violent extremists repeatedly creating new accounts in response to bans, particularly when the names of the new accounts are amended to be subtly different to the original.

In the case of FKD, Telegram routinely banned the channel during the monitored period, however the group repeatedly returned with the same or similar name in order to conduct its activities. This trend may begin to shift in the medium to long term, as FKD's channel administrators grow more frustrated at being continually disrupted.

Figure 36 below is a screenshot of a message from a FKD channel in early March 2022, that explicitly states "we can't make more Telegram recruiting channels because of low reliability". The post complains about repeated moderation efforts, and instead attempts to redirect supporters to a paste site that it was using for recruitment purposes. This was the first instance of Tech Against Terrorism identifying the use of a paste site by FKD.

¹⁷ <https://www.voxpol.eu/download/report/Mapping-the-Jihadist-Information-Ecosystem.pdf>

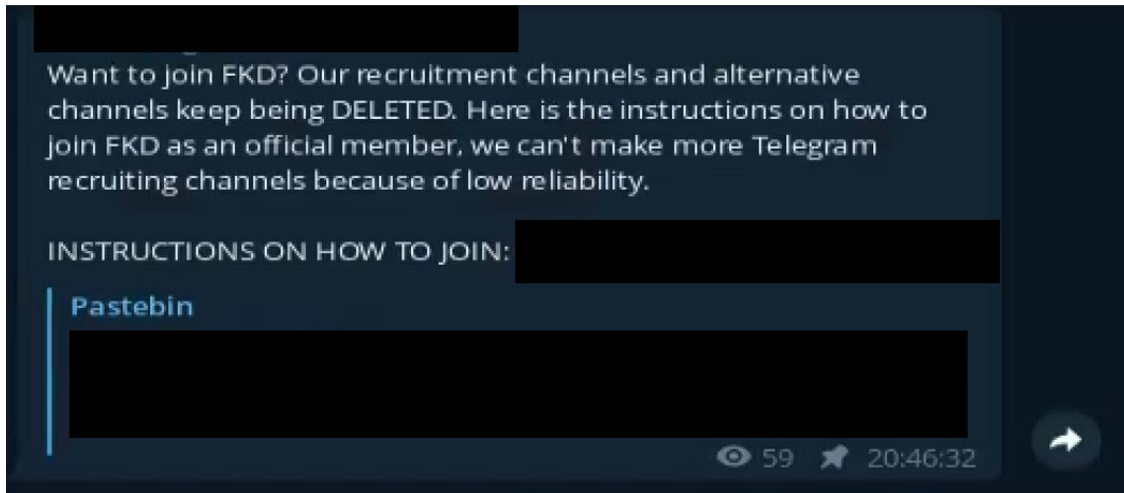


Figure 16. Screenshot of a post by a FKD channel on Telegram. The group complains of repeated takedowns by Telegram's moderators, and attempts to redirect supporters to a content hosting site that the group is using for recruitment purposes.

Like FKD, InJekt Division have been repeatedly de-platformed from Telegram since June 2021, though they have attempted to return to the platform several times since. In January 2022 the group established a new private group. As a means of bypassing Telegram's moderators, the group not only abbreviated their name to "ID," but also included a disclaimer in the description so as to deter moderators. InJekt Division also established an account on encrypted messaging platform Wire, likely in an attempt to diversify their active online spaces due to repeated content moderation.

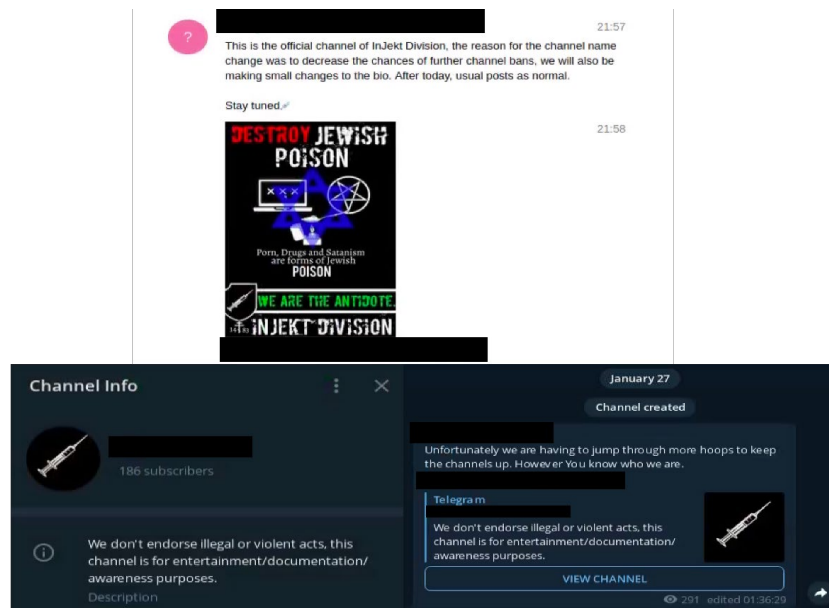


Figure 17. Screenshots of an InJekt Division channel (above) and private group (below) that first appeared in January 2022. This channel actively sought to evade Telegram's content moderation - first by obfuscating its name

to simply "ID", secondly by inserting a disclaimer in the channel description. These behaviours highlight how accelerationist neo-facist actors have sophisticated and elastic methods of evading moderation strategies.

Use of Encrypted Email Services

Tech Against Terrorism identified extensive use of encrypted email services by entities within this new online network, largely for internal communication and the promotion of propaganda content.¹⁸ At its core, end-to-end encrypted (E2EE) email services protect the contents of an email by encoding it, so that it can only be read by the sender and intended recipient.

Much like E2EE messaging platforms like WhatsApp, Signal, and others, E2EE email addresses often provide a greater degree of security as they cannot be as easily hacked as unencrypted email services.¹⁹ When users send a secure email to an address that is not also encrypted instead of receiving the full text, the sender receives a message with a link inviting that person to visit the encrypted email providers' servers to read the encrypted email - which is only readable with the correct password and decrypted locally in the browser.²⁰

E2EE email address providers are used by terrorist and violent extremist actors (TVE) actors from across the ideological spectrum for a number of reasons including, but not limited to:

- They offer a higher degree of security and privacy than unencrypted email providers.
- E2EE emails usually do not require two-factor authentication, meaning TVE actors can repeatedly exploit a provider, even if an affiliated address of theirs had been banned.

The email addresses are usually first promoted by Telegram channels through propaganda posters or in text-based messages in chats, and primarily serve as a point of contact for prospective new members. Despite routine disruptions to email addresses, the entities in this network consistently set up new email addresses either with the same provider, or with a new provider altogether, after they had been deplatformed. Entities would also routinely migrate between using different E2EE email addresses once they had been deplatformed.

The consistent use of E2EE emails by this network is significant, though not a wholly new phenomenon. The actors within the network are likely seeking to diversify their use of the internet, mostly in response to continued disruption on other online spaces. It is likely these entities instrumentalise E2EE emails for a multitude of reasons including internal communication and recruitment, particularly by making it easier for prospective recruits to get in contact off Telegram. This is especially the case if propaganda posters are disseminated in print form offline.

¹⁸<https://www.techagainstterrorism.org/2021/09/07/terrorist-use-of-e2ee-state-of-play-misconceptions-and-mitigation-strategies/>

¹⁹<https://www.pandasecurity.com/en/mediacenter/panda-security/how-to-encrypt-email/#:~:text=Email%20encryption%20is%20the%20process,vulnerable%20when%20sent%20via%20email.>

²⁰<https://www.techagainstterrorism.org/2021/09/07/terrorist-use-of-e2ee-state-of-play-misconceptions-and-mitigation-strategies/>



Figure 18. Examples of promotional propaganda posters that advertised E2EE email addresses linked with the Telegram channel "Tottenwaffen".

Due to ethical and legal reasons, we did not engage with any of these addresses or their administrators, therefore it is unclear precisely what the email addresses provide once contact is made.

Use of Website Infrastructure

We identified widespread use of websites and website infrastructure by this network over the monitoring period. Websites were used for a range of different operational and strategic purposes, including propaganda, archiving, communication and recruitment. Terrorist and violent-extremist operated websites (TVEOWs) have re-surfaced as an important instrument in how TVE actors from across the ideological spectrum use the internet in recent months.²¹

These sites present challenges to tech companies, law enforcement and counterterrorism practitioners alike. This is because the burden of responsibility for removal is not always clearly laid out by law, and TVE actors often find ways of re-establishing websites (usually via changes to top level domain names) after they have been disrupted. Sites exploited by actors within the network would all instrumentalise the same top level domain names, namely: .xyz, .tk, and .eu5.org.

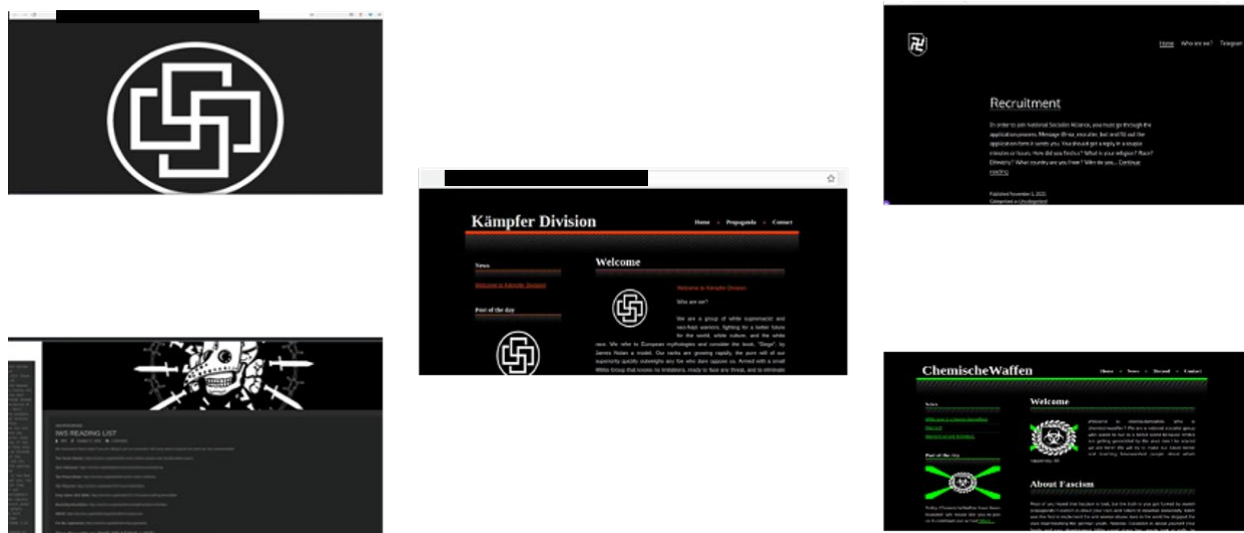


Figure 19: Examples of websites created by entities within the network. At the time of writing, only one of these sites remained live.

Broad improvements in the detection and removal of terrorist content on mainstream social media platforms has broadly pushed such actors onto smaller online spaces in recent years. TVE actors have consequently grown increasingly creative in exploiting the internet, and many have once again returned to relying on websites for their online activities.²²

Tech Against Terrorism identified that two entities within the network - Valknot Division and Wolfwaffen Division - had both established websites in July 2021 using Google Sites, a free web page creation tool offered by Google, much like Wordpress or Wix. Both Google sites were removed following an alert by

²¹<https://www.techagainstterrorism.org/wp-content/uploads/2022/02/The-Threat-of-Terrorist-and-Violent-Extremist-Operated-Websites-Jan-2022.pdf>

²²<https://www.techagainstterrorism.org/wp-content/uploads/2022/02/The-Threat-of-Terrorist-and-Violent-Extremist-Operated-Websites-Jan-2022.pdf>

Tech Against Terrorism in August 2021, after Telegram channels within the network began promoting them on the platform. Neither of these entities had active websites or Telegram channels at the time of writing.

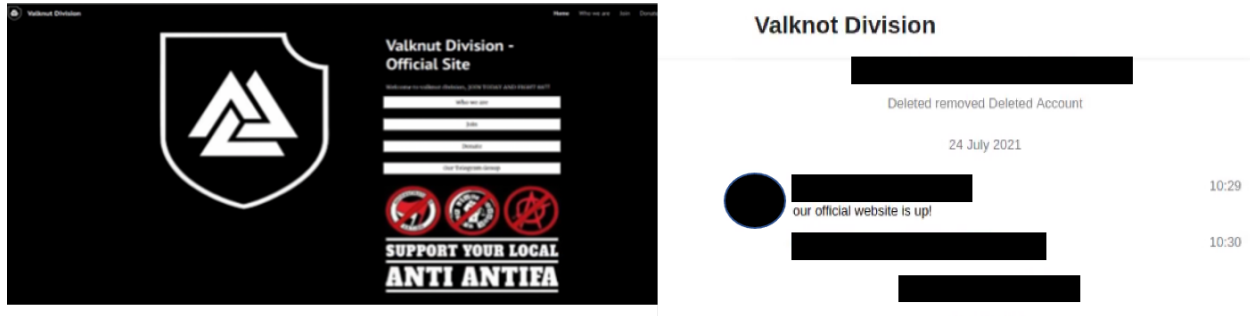


Figure 20. Screenshot depicting Valknut/Valknot Division's use of a Google Site (left) and a post from their Telegram channel that promoted the site in July 2021.

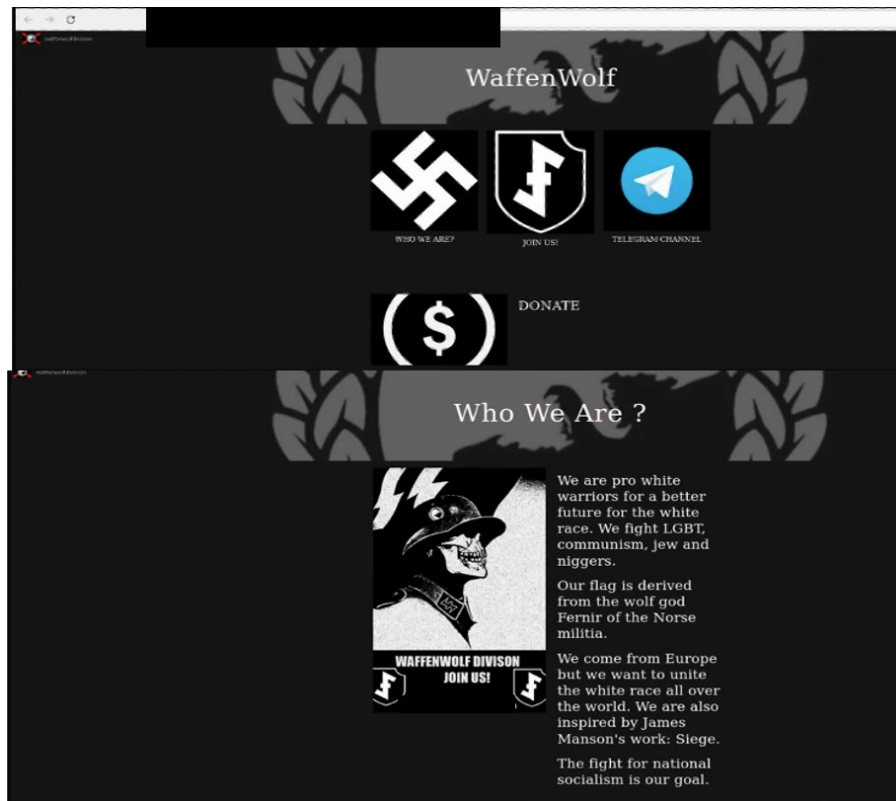


Figure 21. Screenshots of the WaffenWolf Division Google Site that was active in July 2021. The domain was inactive at the time of writing.

Evidence of coordinated behaviour

Tech Against Terrorism identified evidence that suggests that at least three entities within the network were likely to be managed by the same individual or group, as their domains were at one point all hosted on the same IP address. These entities are:

- United Acceleration Front
- National Socialist Alliance
- International White Syndicate

At the time of writing, these domains were all inactive. However, Tech Against Terrorism was able to capture some of the content on two of these sites while they were still live:

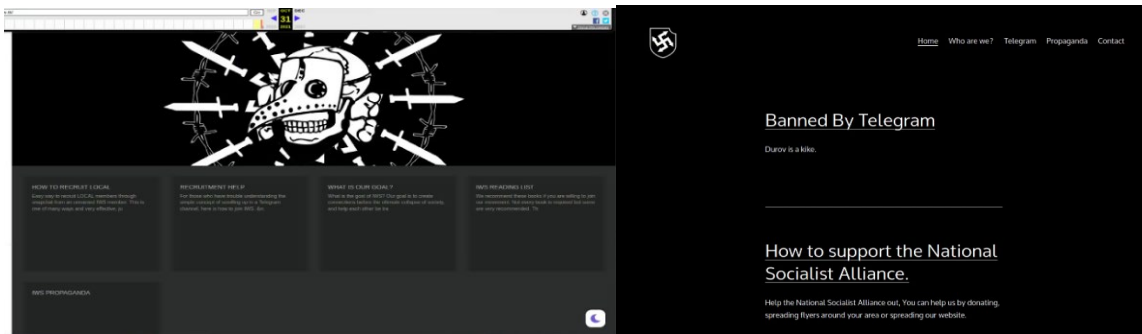


Figure 22. Left: Screenshot of the homepage for a domain linked to the International White Syndicate. Right: Screenshot of the National Socialist Alliance's website homepage. The NSA website changed its top-level domain at least twice from November 2021-January 2022.

HOSTNAME	QUERY TYPE	ADDRESS
www.unitedaccelerationfront	A	[REDACTED]
unitedaccelerationfront	A	[REDACTED]
nationalsocialistalliance	A	[REDACTED]
www.nationalsocialistalliance	A	[REDACTED]
www.internationalws	A	[REDACTED]
internationalws	A	[REDACTED]
cloud.far-right	A	[REDACTED]
www.cloud.far-right	A	[REDACTED]

Figure 23. Multiple websites relating to neo-facist accelerationist entities within this network were all hosted on the same IP address.

Monitoring also identified links to the domain far-right.org, which is now inactive, though at one point appeared to be a directory for militant accelerationist and neo-facist actors online spaces.

Purify, Author at [REDACTED]

This is our first post. We will get started in a couple days posting, Right now we are optimizing some stuff in the background. Please be patient.

[REDACTED] :
Gypsycrusader Sentenced to 3 years in Prison. - [REDACTED]

30 Sept 2021 — Media error: Format(s) not supported or source(s) not found.

[REDACTED] onal-soci... :
List of National Socialist Telegram Groups - [REDACTED]

6 Oct 2021 — List of National Socialist (NatSoc) Groups on Telegram that you can join. [REDACTED]

[REDACTED]
[REDACTED]
Based Websites - [REDACTED]

Based Websites. DailyStormer · StormFront. Search. Search. Archives. October 2021 · September 2021. Far-Right.org | Powered by hate.

Figure 24. Screenshots taken of cached results of far-right.org which was inactive at the time of writing.

It is not immediately clear why an individual or group would create these allied but distinct websites that were part of the same accelerationist neo-fascist network. It is possible that the administrator created multiple sites for seemingly distinct groups in order to exaggerate the size of the movement. This is seemingly done in an attempt to make users believe that the network is more organised and mobilised than it in fact is.

Further investigation is needed into the additional domains hosted on the IP address. The IP address also linked to several other domains relating to extremist far-right ideologies that were all inactive at the time of writing.²³

²³ <https://dns-history.whoisxmlapi.com/lookup-report/0mk8ooz5bM>

Use of Mainstream Social Media Platforms

Monitoring identified that some of the groups within the network sought to exploit mainstream social media platforms such as Instagram, Twitter, Discord, and Snapchat for a variety of strategic and operational purposes, namely the dissemination of propaganda and internal communication.

However, on the whole, the network's exploitation of mainstream online spaces was far less coordinated and persistent than their exploitation of Telegram and website infrastructure. TVE actors from across different ideologies are still drawn to mainstream social media platforms, as these online spaces offer a number of attractive features such as:

- Large audience sizes, which can be useful for recruitment purposes and the dissemination of propaganda content
- Features that are easy to use, such as in-app chats
- Features that allow for rapid content dissemination and archiving

For these reasons, despite continued efforts to counter TVE entities by mainstream social media platforms, terrorists and violent extremists still target these spaces for their online activities. While there was evidence that these actors tried to establish themselves on mainstream online spaces, our teams assessed that the audience reach of these channels was likely to be limited.

Furthermore, there did not appear to be a concerted effort to grow the network's presence on mainstream social media platforms. The reason for this is unclear, however it may have been because entities within the network anticipate removal by content moderators, leading the entities to put little effort into establishing their accounts in mainstream places.

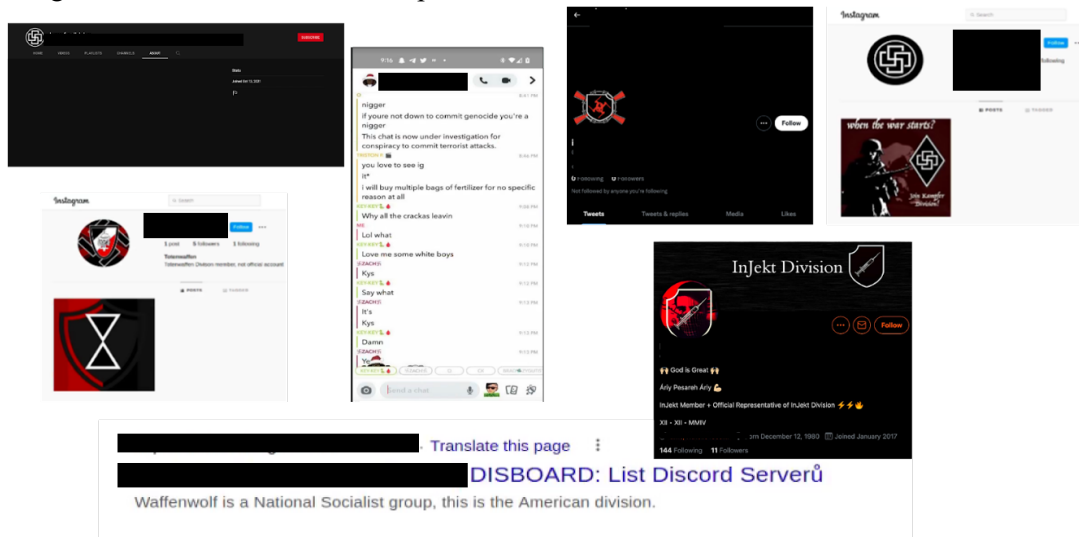


Figure 25. Examples that illustrate how entities within this network sought to exploit mainstream social media platforms including YouTube, Instagram, Twitter, Discord and Snapchat. On the whole, attempts at using these online spaces appeared to be minimal compared to on Telegram. Groups did not attempt to build their profiles or networks on these platforms, and were mostly de-platformed within days/weeks. Following their de-platforming, monitoring did not identify a concerted effort by these actors to return to these mainstream online spaces.