MEDWIN PUBLISHERS
Committed to Create Value for Researchers

Open Access Journal of Criminology Investigation & Justice
ISSN: 3064-7940

Nihilistic Extremist Communities in the Digital Age: Behavioural Characteristics, Online Ecosystems, and Investigative Considerations

Alameen Karim Merali*

Department of Computer Science, University of the People (Student), USA

***Corresponding author:** Alameen Karim Merali, Independent Investigative Researcher, Department of Computer Science, University of the People (Student), USA, **ORCID:** 0009-0000-7933-6532; **emails:** brotheralameen@gmail.com and AlameenMerali@my.uopeople.edu

Conceptual Paper
Volume 4 Issue 1
Received Date: July 03, 2026
Published Date: September 04, 2026
DOI: 10.23880/oajcij-16000135

Abstract

Digital communication technologies have transformed the ways in which extremist ideologies emerge, spread, and interact with broader online ecosystems and this is true especially while existing scholarship has examined violent extremism, cyber-enabled crime, online radicalization and digital investigations independently, we see that comparatively less attention has been devoted to understanding nihilistic extremist communities through an integrated criminological and investigative perspective. This conceptual paper synthesizes literature from digital criminology, cybersecurity, psychology, digital forensics and open-source intelligence (OSINT) to examine behavioural characteristics, communication environments and investigative considerations associated with digitally networked nihilistic extremist communities which rather than focusing on individual investigations or identifiable persons, we see that the paper goes further into examining the recurring themes reported in the scholarly literature including online identity formation, social engineering, platform migration, anonymity, transnational communication and the convergence of extremist ideologies with cyber-enabled criminal activity. The paper concludes by proposing a conceptual framework for analysing investigative challenges, emphasizing evidence preservation, transparent attribution, ethical reporting and interdisciplinary collaboration with its objective being to provide researchers, investigators, educators and policy makers with a structured perspective for understanding emerging online extremist ecosystems while encouraging future empirical investigation.

Keywords: Digital Criminology; Online Extremism; Nihilism; Cybercrime; OSINT; Digital Forensics; Investigative Methodology; Cyber Threat Intelligence

Abbreviations

OSINT: Open-Source Intelligence; HUMINT: Human Intelligence.

CC BY

Chapter 1

Introduction

The emergence of digitally mediated extremist communities has introduced new challenges for criminology, digital investigations, and child protection, especially with groups such as CVLT and 764 which are well-known groups during this time with many of its member targeting children between the ages of 8-17 and above these ages who are vulnerable to their schemes (with others even going up to the age of 25). However, public reporting indicates that 764 didn't operate in isolation as researchers and investigative organizations have described interactions between 764 and other online communities characterized by overlapping membership, shared communication platforms, or similar behavioural patterns through platforms such as Telegram. To understand these groups better, we must better understand why they operate, which isn't for political or religious gain, but rather to show chaos, glorify mass killers and bring forth societal collapse through grooming children and performing extortionate crimes [1,2].

The main problem in reference to these groups is their collaborations with other nihilistic extremist groups that still operate till today, and while public reporting suggests that 764 has fragmented into multiple successor or affiliated online communities at the moment of writing this article, the counterpart groups that were extended from the roots of their origin (being 764) still exist up to now. These groups all form under an umbrella term known as "The Comm," and public reporting has described 'The Comm' as an umbrella term encompassing several online communities that share overlapping membership, culture, or operational characteristics [3] (Institute for Strategic Dialogue, 2025) with these are references for the ties of the Order of the Nine Angles being together with other terrorist groups such as "Atomwaffen Division" as well in multiple articles that exist on the internet, both serving a purpose that exists as a white-only and neo-Nazi extremist group [4,5]. Law enforcement advisories and investigative reporting have documented cases involving the targeting and exploitation of minors and vulnerable adults, especially in law enforcement circles such as the FBI releasing PSAs (Public Service Announcements) and even being reported by other journalists in the OCCRP [6-8]. While taking into consideration their connection within their groups and circles, we must also look into significant problems arising and since the emergence of these communities in the early 2020s, publicly reported tactics and operational practices have continued to evolve [9]. The purpose of this conceptual paper is to synthesize current literature concerning nihilistic extremist communities operating in digital environments and examine their behavioural characteristics, online ecosystems and investigative implications.

This conceptual paper examines nihilistic extremist communities within contemporary digital environments from the perspective of digital criminology with the discussion having its main focus on behavioural characteristics, online communication ecosystems, cyber-enabled criminal convergence and investigative considerations documented within publicly available academic literature, government publications and reputable investigative reporting. However, the paper doesn't seek to investigate or determine the criminal responsibility of any individual or organization but rather that it synthesizes existing knowledge to provide a structured conceptual understanding of how digitally networked nihilistic extremist communities operate and the challenges they present to researchers, investigators, and policy makers.

The continued evolution of online extremist communities presents significant challenges for criminology, cybersecurity and digital investigations with digital platforms having enabled geographically dispersed individuals to communicate, recruit, share information and exploit technological infrastructures across national boundaries especially through the use of encryption chat messengers such as Telegram and as these online ecosystems evolve, investigators must navigate issues relating to digital evidence preservation, attribution, cross-jurisdictional investigations, encryption and rapidly changing communication platforms [10]. By integrating concepts from digital criminology, digital forensics, cybersecurity and open-source intelligence, we understand that this paper seeks to contribute to a broader understanding of the behavioural and technological characteristics associated with nihilistic extremist communities as it also highlights areas where further empirical research may improve investigative methodologies, interdisciplinary collaboration and evidence-based policy development.

This paper is organized into eight chapters.

- Chapter One introduces the topic, outlines the problem statement, defines the scope of the paper and explains its significance.
- Chapter Two reviews the conceptual foundations of digital criminology, online extremism and related disciplines to establish the theoretical context for the discussion.
- Chapter Three examines behavioural characteristics commonly identified within the literature concerning digitally mediated nihilistic extremist communities.
- Chapter Four explores the digital ecosystems in which these communities communicate, interact and adapt to technological change.
- Chapter Five discusses documented intersections

Copyright© Alameen Karim Merali.

between extremist communities and cyber-enabled criminal activities reported within existing research and public sources.

- Chapter Six examines investigative considerations which includes digital evidence preservation, attribution challenges, open-source intelligence, ethical reporting and cross-jurisdictional investigations.
- Chapter Seven identifies limitations in the current body of knowledge and proposes directions for future research.
- Chapter Eight concludes the paper by summarizing the principal conceptual themes and discussing their implications for researchers, investigators and policy makers.

Chapter 2

Conceptual Foundations

Digital criminology serves as a macro-framework that examines how rapid technological advancements have fundamentally altered the commission of crime, the structure of victimization as well as an institutional response on the justice system with systematic shifts that explain how infrastructures go from using end-to-end encryption to decentralized network hosting and automated data processing which redefine the spatial dynamics for offending. Inclusive to this, we will see that within this study, the traditional physical environments are replaced with virtual spaces that allow for offenses such as targeted online harassment as well as systematic swatting campaigns with digital criminology goes beyond analysing how the state, legislative bodies and global policing organizations can adapt their legal frameworks in order to perform punitive measures to enforce order within the non-physical domain [15].

The cyber-criminology here focuses on the behavioural micro-dynamics of the offender within the virtual environment, which is then paired with the technological mechanisms employed to mitigate, detect, and investigate these offenses as opportunities for offending continue to increase, cyber-criminology helps analyse how these structural features such as anonymity, asynchronous communication and transnational connectivity can help create new opportunities for criminal behaviours. Furthermore, we see that this perspective is highly relevant when evaluating nihilistic extremist communities as these groups don't rely on local physical cells but rather exploit digital infrastructure in order to aggregate, communicate and coordinate highly damaging activities through cross-border means and it models how victimisation occurs online as the internet architecture allows such aggressive threat actors to systematically target, profile and exploit vulnerable individuals globally without having to establish a physical presence [13].

Online extremism represents a deliberate manipulation and weaponization of the digital platforms in order to disseminate radical ideologies designed to influence, radicalise or mobilise vulnerable individuals towards harmful beliefs and actions which further undermines democratic principles, the rule of law, individual liberty and mutual tolerance by promoting systematic hatred, violence and social fragmentation. To add up, digital platforms provide a highly optimized environment whereby individuals from around the world can cluster into ideological echo chambers and these spaces can reinforce extreme beliefs that rapidly share harmful criminal methodologies. The jurisdictional complexity behind this lies on the velocity and anonymity of the digital communication which exponentially complicates the ability for law enforcement to identify, disrupt or prosecute actors who coordinate across multiple international jurisdictions [14].

Nihilistic ideology relies on a philosophical framework that denies or rejects the foundational aspects of human existence, objective meaning, morality as well as established reality by deconstructing traditional motivation through criminal intent because rather than operating for material acquisition, financial profit or a desire to install a new political or religious order, the nihilistic actor operates on the premise of deconstruction for its own sake. Inclusive to this, we see that such an ideology provides the conceptual lens needed to analyse online subcultures that view social structures as fundamentally broken, terminal or artificial which when integrated into a digital environment, we see that the nihilistic world views merge with online clout dynamics which turn destructive actions and symbolic violence into primary methods of building an identity and gaining status within extremist groups [12].

Cyber-enabled crimes are a distinctive category of offenses that are traditional in nature such as fraud, extortion, theft and harassment but are executed at a massive scale, speed and scope due to the utilization of information and communication technology. It encompasses the use of phishing pipelines, infostealers to compromise systems and unlike standard cybercriminals who deploy ransomware and cryptojacking malware for financial gain, nihilistic extremist groups utilize these methodologies as tools for radicalisation, psychological coercion and institutional sabotage with cyber enabled tools such as remote access trojans and doxxing being systematically deployed to gain control over victims, which then transforms digital leverage into severe real-world harm [10].

Copyright© Alameen Karim Merali.

Finally, we have digital investigations, which encompass the systematic collection, forensic analysis and legal preservation of electronic data to uncover verifiable evidence related to cyber-dependent and cyber-enabled offenses, which by forensically examining the volatile memory, network traffic registries and metadata, it can be used by investigators to trace the origin, pathway and techniques used by the threat actor to confirm their attribution. When it comes to investigating nihilistic extremist groups, it requires a complete departure from standard cybercrime investigative protocols as conventional forensics typically follow a clear financial trail or transaction log and because nihilistic threat networks are highly decentralized, fluid and non-monetary, it means that digital investigators will have to pivot to tracking the fragments of ideological footprints, indicators of destructive intent, encrypted peer-to-peer metadata and highly volatile anti-forensic environments [11].

Chapter 3

Behavioural Characteristics

Federal and law enforcement agencies such as the FBI and the U.S. Department of Justice classify these networks as the Nihilistic Violent Extremist Groups with their primary objective being the systematic societal disruption which is achieved by driving vulnerable youth toward real-world violence, self-harm and severe digital exploitation [16,17]. The identity formation began as members of these groups began to seek out adolescents experiencing severe social isolation, mental struggles and identity crises through gaming servers such as Minecraft and Roblox [18,19]. The recruits of such groups are conditioned to adopt a bleak and anti-social worldview which then reframes themselves from being "isolated victims" into being elite digital operators who stand above the standard moral rules [20].

Cohesion within the CVLT, 764 and the offshoots such as Harm Nation is maintained by the use of extreme gore imagery, animal torture as well as the evidence of the presence of self-harm from victims of extortion [21,22]. This group cohesion then brings forth status, respect and ranks within these decentralized groups which they earn by documenting and sharing the escalating attacks that they perform either in the real world or through performing digital damage [23]. Their algorithmic breadcrumbs are such that traditional ideological recruitments are done through users being funnelled from public gaming spaces or meme boards into private direct messaging or encrypted messaging services such as Discord and Telegram [18].

This then leads to desensitization of the recruit through the use of dark humour and subculture aesthetics which then slowly begin to escalate into extreme violence and explicit content to lower the recruits' moral barriers [18]. Social engineering becomes relevant when these predators begin to pose as peers and protectors or show to have romantic interests in order to gain trust and gather personally identifiable information and explicit content from the victim which is then used to perform intense blackmail, swatting threats and psychological coercion against a victim [19]. Victims are then given the understanding that them, the society and their families are worthless or artificial, framing them as some kind of non-playable characters, which subsequently reduced empathy toward those who had suffered harm and brings forth the ability to force victims to carve the group names or symbols into their skins as functions of a psychological ritual of passage into their group, which normalizes self-mutilation as a standard metric of devotion to the group [24].

Their digital identities are formed through fluid pseudonyms especially with leaders from 764 such as Bradley Cadenhead who went by the alias of Felix and the subgroup operators such as "War" and "Trippy" who continuously rotated aliases, burner accounts and decentralized servers to evade law enforcement detections and platform bans [25]. However, nowadays, their Operational security considerations are relatively weak as they can livestream exposing their voices which eventually exposes their accents which could be used to identify where they're from, and other operational security mistakes that take place in the current era of the groups that operate. Inclusive to this, exposure of information such as their usernames, social media accounts and the similar lead to consequential operational security failures which can result in the perpetrators being more readily identified.

Chapter 4

Digital Ecosystems

Digital ecosystems refer to interconnected online platforms that enable communication, social interaction, content sharing and community formation. Contemporary online extremist communities frequently operate across multiple digital ecosystems rather than relying upon a single platform which allows them to adapt to moderation efforts, diversify communication channels and reduce disruption. While encrypted messaging platforms such as Telegram has been referenced by law enforcement advisories to find cyber-criminals integrated within the nihilistic extremist community because of the use of encryption to help hide their identity while performing their work, these observations suggest that encrypted communication platforms may facilitate identity formation, community cohesion and the pursuit of status or recognition within certain online extremist communities [26].

Copyright© Alameen Karim Merali.

Cross-platform migrations between encrypted and unencrypted messaging services connected to gaming services is commonly observed by researchers as well, in which we see that public reporting has described gaming platforms and community-oriented communication services such as Roblox and Discord as environments where initial contact may occur before communication migrates to encrypted messaging platforms and that public reporting has also documented cases in which victims were initially contacted on one platform before communication migrated to encrypted messaging services, which is where coercion, exploitation or extortion allegedly escalated [27].

At some point, it could get extreme to the point that the victim may be extorted to perform activities that are otherwise considered illegal and inappropriate for the relevant audience, as public reporting suggests and these nihilists can then get these victims to add them on their social media platforms to facilitate further exploitation, coercion or other forms of cyber-enabled offending out of the ordinary encrypted platforms [28]. We can finally see that digital ecosystems present to us more than communication technologies as they constitute of interconnected environments that facilitate community formation, information exchange and behavioural adaptation and understanding how online extremist communities migrate across platforms is important for digital investigations because evidence is often distributed across multiple services, jurisdictions and technological environments.

Chapter 5

Criminal Convergence

Peer-reviewed reports indicate the demonstration of financial fraud within the com is structurally tied to account takeovers with investigative reporting and court records having documented the involvement of some members in cyber-enabled financial offences, including fraud, credential theft and account compromise, although the prevalence and organizational role of these activities across the broader community remain areas requiring further empirical study. These kinds of fraud are heavily used to fund "clout-driven" lifestyles whereby the funds are used to purchase expensive digital assets, automated botting tools and custom infrastructure that can be used to boost standing within the groups [20,21,22].

When it comes to cases whereby coercion occurs, documented case files show that compromised minors who would be victims of sextortion are used to execute low-level financial fraud such as using their parents' credit card to fund the group's infrastructure or purchase them digital items. Identity harvesting through the use of social engineering led to credential theft whereby personally identifiable information and other sensitive information may be stolen such as passwords, usernames and so on with methodologies such as getting victims to livestream their phones and gain access to such information during the livestream [28]. Access to a victim's account is then utilized by the com actors which can then be further used to harvest real-world identities, locate family members and perform doxxing and swatting [29].

Social engineering represents a significant threat in this context, particularly when used for asymmetric psychological manipulation of the victim may take place which creates a gap between digital intrusion and physical harm, through the use of tactical pretexting, operators of such groups profile vulnerable targets by utilizing highly sophisticated "peer-empathy" to build swift and intense emotional attachments and once the trust has been established then the actor pivots to aggressive manipulation including extracting explicit imagery, creating AI deepfakes, forcing their targets into video calls and similar techniques. In terms of malware distribution, research shows that these groups don't typically develop zero-day exploits but rather rely on commodity malware such as remote access trojans, info stealers and keyloggers which can be obtained through cybercrime forums or open-source repositories. This malware is then distributed as a trojan through game modifications, cracked software utilities and direct file transfers over Discord or Telegram to disguise media. This malware is then deployed on victims' machines to capture real-time data, record keystrokes and provide the actor with complete surveillance [28,32].

The convergence of financial crime, cyber-enabled offending, psychological manipulation and digital exploitation illustrates that contemporary nihilistic extremist communities shouldn't be understood as operating within a single criminal domain but rather that the literature suggests that these communities exhibit characteristics of hybrid criminal ecosystems in which ideological narratives, cybercrime, social engineering, financial offending and digital exploitation that reinforce one another. This convergence presents significant challenges for investigators because individual offences are often interconnected, requiring multidisciplinary investigative approaches that integrate digital forensics, behavioural analysis, financial investigations and intelligence collection.

Chapter 6

Investigative Considerations

When it comes to preserving digital evidence especially when it comes to cybercrime that goes to this extent, we

Copyright© Alameen Karim Merali.

need to consider that cases that reference Child Sexual Abuse Material must be handled with caution, including the review of laws of certain jurisdictions of where the act has taken place, and through the proper channels [33,34]. For illustrative purposes, consider a scenario in which if the crime is happening between a victim from the Netherlands and the suspect is from the United States then the laws from both countries and states must be checked to make sure of what kind of action must be taken during investigation. Also, because the possession, handling and transfer of CSAM is heavily regulated in many jurisdictions, with limited exceptions that may apply to authorized law enforcement personnel, forensic examiners or other individuals acting under applicable legal authority. However, when it comes to other forms of evidence that can be captured during the investigation, it's necessary to make sure that screenshots aren't included in there because screenshots may be admissible in some jurisdictions, but their evidentiary value often depends on authentication, metadata, integrity verification and chain-of-custody documentation [35-38].

Where technically and legally appropriate, investigators may preserve dynamic online activity through contemporaneous recording or other forensic acquisition methods, while ensuring that evidence is collected, authenticated and preserved in accordance with applicable legal and forensic standards, with proper hashing to ensure integrity of the evidence isn't impacted, with digital evidence being documented and managed in accordance with applicable organizational procedures and legal requirements while maintaining an auditable chain of custody [29,31]. Open-Source Intelligence (OSINT) represents an important investigative consideration within digital investigations because it enables investigators to analyse publicly available information from multiple online sources to support attribution and contextual understanding with publicly accessible information associated with usernames, email addresses, telephone numbers, social media profiles and other digital identifiers which may contribute to the reconstruction of online activities and the identification of relationships between digital identities. Within investigations involving digitally mediated extremist communities, we see that OSINT may therefore assist investigators in correlating fragmented information across multiple platforms, therefore supporting attribution while complementing other forms of digital evidence rather than replacing them. Other methods of attribution include methods such as stylometric analysis, whereby the writing of the suspect is compared with other suspected identities tied to the suspect to find out if it's them that's actually behind a suspected identity.

Typing and writing patterns can contribute to stylometric analysis. While a person can be able to change their stylometry slightly, they can't do it completely as Each individual has a distinct writing style and approach to expression. However, reports show that stylometry is normally used for probabilistic predictions for a suspect and shouldn't be considered absolute proof, but rather can be used as supporting evidence [40,41]. When it comes to reporting, it's necessary to understand that anything that's documented as evidence should have a classification to it, in most cases, access to sensitive investigative material should be restricted in accordance with applicable legal, organizational and evidentiary requirements and only approved to be seen by people who are named in the chain-of-custody documentation till the documents reach court and until disclosure is authorized in accordance with applicable legal processes. In reference to anything that requires cross-jurisdictional investigations, reviewing of the necessary MLAT, laws and treaties that apply between the two jurisdictions is necessary to determine the point of how an investigation should be conducted [38,39]. The use of tools across different jurisdictions should also be taken into consideration when conducting investigations.

Chapter 7

Future Research Directions

As technology develops, there's a continuous transformation between operational methodologies of the criminal networks and the digitally mediated extremist communities with threat environments leveraging advanced digital tools to scale their operations and obscure their identities [42,43]. This can cause investigative work to keep pace with the behavioural adaptations performed by offenders that utilize digital platforms. Emerging generative AI provides advanced image creation technologies which have shifted the barrier for generating synthetic digital content and this advancement itself has brought forth the ability to create synthetic harmful content with the challenge being that that influx of the image being synthetic, which complicates traditional victim identification and evidence verification workflows for the authorities [44].

Intelligence augmentation through the usage of AI systems may assist investigators in analysing large volumes of digital information by identifying patterns, correlating publicly available data and prioritising investigative leads through advanced machine learning algorithms that can automate the correlation of vast amounts of publicly available information to provide actionable investigative leads with an ethical consideration being that stringent legal frameworks and ethical safeguards on privacy and data collection, which are necessary to be considered [45]. We observe the use of passive reconnaissance through OSINT methodologies that focus on non-intrusive and passive investigative processes that map networks without alerting targets, especially if

Copyright© Alameen Karim Merali.

performed through automated means, with the challenge here being that it may require the integration of other traditional intelligence gathering disciplines such as the use of Human Intelligence (HUMINT) and the use of Confidential Informants to validate AI generated leads.

Behavioural considerations especially with digitally mediated extremist communities and offender networks that monitor law enforcement capabilities and exhibit high levels of counter-surveillance awareness is necessary to take into consideration because As investigative methodologies continue to advance, future research should also examine how digitally mediated extremist communities adapt their operational security and communication practices in response to evolving investigative capabilities. Future research on the behavioural modelling of such groups needs to be examined according to how advances in AI help influence the real-time behavioural adaptations and operational security of these networks [46]. With the proliferation of real-time streaming technologies, there are introductions of new environments for digital evidence collection as the impact on the offender's behavior shows their interaction patterns with investigations on the dynamics that create unique investigative opportunities that necessitate the rise of agile investigative models that are capable of real-time evidence preservation [47].

Chapter 8

Conclusion

This paper provides a comprehensive and multidisciplinary criminological examination of contemporary online nihilistic violent extremist communities with the main focus being on the decentralized and clout-driven subcultures identified as "The Com" and its constituent networks such as 764 and CVLT, By synthesizing digital criminology with traditional behavioural frameworks, we can see that this study fills a critical gap in existing literature which has historically struggled to classify and analyse threat actors who operate outside conventional ideological, political or financial paradigms [48]. The conceptual contribution of this paper is the proposal of a nihilistic digital accelerationism framework, which may help explain how status seeking, destructive online subcultures, cyber-enabled exploitation, and accelerationist narratives converge within decentralized digital extremist ecosystems. Also, while traditional criminology and counter-terrorism models are fundamentally built on rational-choice theories or structured ideological frameworks, the primary objective of the nihilistic extremist networks in this fashion is to cause systematic destruction, chaos and institutional erosion for its own sake, as it is further fuelled by intense social anomie and mediated through an online subculture that rewards severe harm with a digital status [49].

Furthermore, the paper has advanced the understanding of criminal convergence within decentralized spaces whereby it has mapped how these actors don't merely utilize the internet as a method of passive communication but rather to weaponize its structural characteristics such as anonymity, pseudonymity, end-to-end encryption and algorithmic discovery pathways, in such a way that merges traditional criminal offenses with sophisticated digital actions [50]. Also, by further analysing the intersection of cyber-enabled crimes such as doxxing and malware distribution with severe interpersonal exploitation such as swatting and extortion, this study illustrates how digital leverage is systematically transformed into real-world physical and psychological trauma. Finally, the study has also re-evaluated limits to traditional forensic methodologies as it underscores that when investigating decentralized, atomized and fluid networks, the conventional strategy of 'following the money' may be insufficient when financial gain is not the primary driver but the paper therefore establishes a conceptual foundation for forensic practices that prioritize the extraction of volatile digital artifacts, metadata correlation and the tracking of distinct ideological footprints [51].

References

1. The Frightening Reality of Online Predators (2026) Central District of Illinois, United States Department of Justice, USA.
2. (2026) FBI Warns Of Extremist Networks Targeting Children Through Online Games. Votp News.
3. (2026) Com/764: Transnational Abuse, Extortion, and Cybercrime Networks Targeting Youth, Canadian Anti-Hate Network.
4. (2025) A Victim-Centric Resource on the 764 Network, Institute of Strategic Dialogue. Networks of Harm.
5. Mapping Militants Project (MMP) (2022) Order of Nine Angles.
6. (2025) Violent Online Networks Target Vulnerable and Underage Populations Across the United States and Around the Globe, Internet Crime Complaint Centre.
7. Benedetto ED (2025) FBI Warns of Online Groups Forcing Minors into Self-Harm, Explicit Content, and Suicide. OCCRP.
8. Koroleva A (2025) FBI Cracks Down on Child Predator Network '764'. Organized Crime and Corruption Reporting Project (OCCRP).

Copyright© Alameen Karim Merali.

9. (2025) 764 Anti-Defamation League, Centre of Extremism. ADL.
10. Alvarez R (2021) Cyber Enabled Crime vs. Cyber Dependent Crime. IP Investigations and Protection Blog. IP Probe-Blog.
11. Bakersfield Forensics. What Are Digital Investigations and Why Are They Important?. AMR Digital Forensics.
12. Cumberland D (2026) What Is Nihilism? Types, Key Thinkers, and Finding Meaning Beyond It. The Meaning Movement.
13. (2025) What is Cybercriminology? Understanding the Intersection of Technology and Criminal Justice. Kent State University, USA.
14. Lally C, Bermingham R (2020) Online extremism. Parliamentary Office of Science and Technology (POST), Parliament of the United Kingdom.
15. (2025) Digital criminology-Department of Criminology and Sociology of Law (IKRS). University of Oslo, Norway.
16. Setera K (2026) Federal Bureau of Investigation, FBI Boston Warns of Nihilistic Violent Extremists Targeting Children and Vulnerable Victims Online. FBI.
17. Nash K (2026) Violent Extremist Network "764" Member Sentenced to 30 Years for Sexually Exploiting Minors And Cyberstalking. United States Department of Justice, USA.
18. Levine M (2026) Parents of 764 victim file wrongful death lawsuit against Discord. ABC News.
19. Murphy M (2026) The Cyberbullies of 764 Torment Teen Girls as Blood Sport. Bloomberg.
20. (2025) Violent online groups exploiting children and youth. Royal Canadian Mounted Police.
21. Winston A (2024) There Are Dark Corners of the Internet. Then There's 764. WIRED.
22. (2025) '764' Extremist Group Leader Pleads Guilty to RICO, Child Exploitation Charges. Office of Public Affairs United States Department of Justice.
23. Clifford B (2026) 'Nihilistic Violent Extremism' Isn't a Thing, and I'm Tired of Pretending It Is. Lawfare.
24. Macharia R (2024) CTC SENTINEL Report. Combating Terrorism Centre.
25. Fiscus K (2026) Nashville FBI office warns of violent online group targeting kids. Tennessean.
26. (2025) Networks of harm: A victim-centric resource on the 764 network. Institute for Strategic Dialogue.
27. Perets S (2026) Terror groups groom and recruit children online, exploiting Roblox, Discord, and Minecraft-NYT. The Jerusalem Post.
28. (2023) Shields Up: Protecting against cyber threats. CISA.
29. (2021) Guidelines for digital forensics first responders. INTERPOL.
30. (2020) Security and privacy controls for information systems and organizations. National Institute of Standards and Technology.
31. Guttman B, White DR, Williams S, Walraven T (2022) Digital evidence: Considerations for Evidence Handlers. NIST Interagency.
32. Roy SS, Vafa EP, Khanmohammadi K, Nilizadeh S (2024) DarkGram: A large-scale analysis of cybercriminal activity channels on Telegram. arXiv.
33. (2025) CyberTipline. National Centre for Missing & Exploited Children.
34. (2026) How to report online child sexual exploitation and abuse. US Department of Homeland Security.
35. (2020) SWGDE guidelines for video evidence canvassing and collection. Scientific Working Group on Digital Evidence.
36. (2024) Standard guide for forensic digital image management. OSAC National Institute of Standards and Technology.
37. Greco C, Ianni M, Guzzo A, Fortino G (2025) A digital forensics approach for validating screen evidence. CEUR Workshop Proceedings.
38. (2022) Mutual legal assistance treaties of the United States. US Department of Justice, USA, pp: 1-8.
39. 24/7 Network established under the Convention on Cybercrime. Council of Europe, France.
40. Rexha A, Klampfl S, Kröll M, Kern R (2018) Authorship identification of documents with high content similarity. Scientometrics 115: 223-237.
41. Kumarage T, Liu H (2023) Neural authorship attribution: Stylometric analysis on large language models. Proceedings/Elsevier record.
42. (2025) 25 arrested in global hit against AI-generated

Copyright© Alameen Karim Merali.

child sexual abuse material. Europol.

43. (2025) CyberTipline data. National Center for Missing & Exploited Children.

44. Ciardha CO, Buckley J, Portnoff RS (2026) AI-generated child sexual abuse material: What's the harm? AI & Society.

45. (2026) Generative AI: A new threat for online child sexual exploitation and abuse. United Nations Interregional Crime and Justice Research Institute, Italy.

46. (2024) Child sexual abuse material created by generative AI and similar online tools is illegal. US Department of Justice.

47. Daviess B (2026) 764 and The Com: Misconceptions and guidance. CNA.

48. Argentino MA, Lindsay A (2026) Remotely coerced violence: 764, The Com Network, and the hybridization of threats. Combating Terrorism Center at West Point 19(6).

49. Beck P, Hughes S, Ware J (2026) Lawfare Daily: "I'm angry that I exist": Nihilistic violent extremism with Seamus Hughes and Jacob Ware. Lawfare.

50. Bellaiche J, Comerford M, Rose H (2026) Beyond extremism: Platform responses to online subcultures of nihilistic violence. Global Network on Extremism and Technology. King's College London, United Kingdom, pp: 1-32.

51. (2025) Leaders of 764 arrested and charged for operating global child exploitation enterprise. US Department of Justice, United States.

Copyright© Alameen Karim Merali.