

TLP CLEAR – DISSEMINATION UNLIMITED



(TLP-C) CHILD ATTACKERS GETTING YOUNGER AS U.S. BORN ONLINE NIHILIST NETWORKS GO GLOBAL, (AX) 23 OCT 2026

KNOW THE TARGET – WATCH THE TARGET – LOOK DEEPER -EXPECT THE UNEXPECTED
Matthew 11:12 "And from the days of John the Baptist until now the kingdom of heaven suffereth violence, and the violent take it by force."

IN OBSCURA THEAT LEVEL – IMMINENT

CAVEAT: THIS INTELLIGENCE PRODUCT RELIES ON OPEN-SOURCE MEDIA OR GOVERNMENT RELEASED UNCLASSIFIED INFORMATION. RECOMMENDED ACTIONS ARE INCLUDED FOR CLIENTS FOR INFORMATION AND ACTIONS DEEMED APPROPRIATE.



IN OBSCURA CONTEXT

The threat environment emphasized in my threat intelligence reporting and analysis focuses on churches, congregations and clergy as targets. These targets have and will experience an escalating operational tempo, also based on a body of In Obscura reporting. The indoctrination and resultant polarization of American youth also as targets of inimical domestic and foreign subversive and terror groups have realized a measure of success. The now historic mobilization of LGBTQ mass shootings and attacks is one such manifestation. The second is the global reach by the 764 Group and with a growing preponderance with Satanism. Numerous vectors have and will affect Christians, Clergy and Church Security Teams are advised strongly to know and understand the threats and take appropriate proactive approaches to detect, deter, defend and destroy attacks and pre-operational surveillance.

RESTRICTED - PROPRIETARY INFORMATION. The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBSCURA, LLC. RESTRICTED FROM DISCLOSURE // NOT FOR PUBLIC RELEASE OR NEWS MEDIA

TLP CLEAR – IN OBSCURA CAVEATS APPLY

INTEL REPORT

Child Attackers Are Getting Younger as U.S.-Born Online Nihilist Networks Go Global, American Kinetix, Early Bird Intelligence Brief for 23 Oct 26, Intel Report Section, americankx.com

WHAT IS THIS REPORT ABOUT?

Loosely organized online networks that glorify violence for its own sake are pulling in children and pushing more of them toward attacks. The two main strands are the Com network, including 764, which coerces minors into self-harm, sexual exploitation and violence, and the True Crime Community (TCC), which venerates past school shooters and encourages imitation. It matters operationally because the threat began in the United States, recruits entirely online, and is now producing school attacks by children as young as 12 on several continents.

BOTTOM LINE UP FRONT

Nihilistic violent extremism (NVE) is now a top FBI domestic terrorism priority, and the attacker pool is getting younger. The FBI reported more than 350 subjects tied to 764 and related networks across all 56 field offices by early 2026, and NVE case openings are still climbing. At least six school attacks or attempts abroad by children aged 12 to 16 since May 2026 show the model spreading worldwide. With minors on both sides and radicalization running through U.S.-owned platforms, the decisive levers are early identification, platform cooperation and allied information sharing.

KEY JUDGMENTS

RESTRICTED - PROPRIETARY INFORMATION. The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBSCURA, LLC. RESTRICTED FROM DISCLOSURE // NOT FOR PUBLIC RELEASE OR NEWS MEDIA

TLP CLEAR – IN OBSCURA CAVEATS APPLY

TLP CLEAR – DISSEMINATION UNLIMITED

- We assess that NVE networks are a sustained homeland threat to U.S. schools and minors. FBI caseload growth, the overseas attack pattern and falling attacker age all point the same way.
- The United States is both the origin and the main exporter of this threat, which gives Washington responsibility and leverage over the platforms that carry it.
- These offenders mix grievance, often bullying, with imitation of past shooters and leave few classic warning signs. A relative's firearm enabled at least three of the 2026 attacks abroad.
- We expect attacker ages to keep falling and copycat attempts to spike after each publicized attack.
- The evidence is uneven. FBI figures are official, but global incident counts and age trends rest on unverified research, calls for a public health model are advocacy, and not every attack below has a confirmed network link.

SITUATION REPORT

The Com network is a loose ecosystem of groups, including 764, Maniac Murder Cult and No Lives Matter, that groom children into self-harm, sexual exploitation and violence. The TCC celebrates past shooters, and violent members urge each other to imitate them. Ideology is borrowed piecemeal from neo-Nazism, ISIS propaganda and misogyny; online status is the real reward. Recruitment runs through mainstream social media, Telegram and gaming platforms such as Roblox and Discord, and can take days.

What changed in 2026 is the age and spread of attackers.

1. A 13-year-old shot dead two staff members at a school in Rio Branco, Brazil, on 5 May.

RESTRICTED - PROPRIETARY INFORMATION. The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBSCURA, LLC. RESTRICTED FROM DISCLOSURE // NOT FOR PUBLIC RELEASE OR NEWS MEDIA

TLP CLEAR – IN OBSCURA CAVEATS APPLY

TLP CLEAR – DISSEMINATION UNLIMITED

2. A 12-year-old in San Vito Lo Capo, Sicily, tried to knife his teacher while streaming it on Telegram on 29 May.
3. Two students aged 14 and 15 killed three fellow students in Tacloban, Philippines, on 22 June.
4. A 14-year-old killed his grandparents and then school staff outside Bangkok on 7 August.
5. A 14-year-old shot his principal and a teacher in Aubagne, France, on 12 October; antiterrorism prosecutors took the case over signs of TCC affiliation.
6. A 16-year-old stabbed a six-year-old girl at a school in Umhlali, South Africa, on 13 October.
7. Indonesian counterterrorism authorities referred 620 children exposed to violent online extremism, with the TCC a named concern, for intervention in the first eight months of 2026.

At home, the FBI went from about 250 investigations linked to 764 in May 2025 to more than 350 subjects by February 2026. It reported a roughly 300 percent rise in new domestic terrorism cases in 2025, much of it NVE, and an 85 percent rise in NVE cases in 2026.

COURSES OF ACTION

Most Likely

Incidents continue at the current pace, with plots disrupted in the United States and Europe and attacks by younger offenders elsewhere. Steady FBI subject counts, more juvenile federal prosecutions and arrests that follow tips rather than attacks would confirm this path.

Most Dangerous

A high-casualty attack livestreamed by an American minor sets off imitators at U.S. schools within days, possibly with 764-style coercion pushing a groomed victim to act. Watch for online praise of the 2026 attackers, post-incident

RESTRICTED - PROPRIETARY INFORMATION. The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBSCURA, LLC. RESTRICTED FROM DISCLOSURE // NOT FOR PUBLIC RELEASE OR NEWS MEDIA

TLP CLEAR – IN OBSCURA CAVEATS APPLY

TLP CLEAR – DISSEMINATION UNLIMITED

spikes in school threats, and network members abroad directing American children.

Least Likely

The networks fade as platform enforcement and arrests break their cohesion. That would require sustained takedowns, falling FBI case openings and proof the groups can no longer rebuild under new names.

IMPACT ON USA

U.S. national security: NVE is a top FBI domestic terrorism priority and draws Joint Terrorism Task Force resources.

U.S. foreign policy: Allies facing a U.S.-born threat will seek U.S. data and platform access, giving Washington leverage to deepen counterterrorism partnerships on its terms.

Domestic effects: Expect pressure on Congress and the states over platform liability, age verification and safe firearm storage.

American citizens or organizations: U.S. schools, parents and minors are the primary targets, and U.S. social media and gaming companies face legal and reputational exposure.

CONCLUSION

The evidence converges on younger attackers and more copycats: U.S. case counts are rising and children aged 12 to 16 are carrying out school attacks on several continents. The assessment would ease if FBI case openings flattened, platforms showed sustained removal of these networks, and the 2026 overseas pattern did not reach U.S. schools. It would harden with a U.S. school attack tied to these networks or evidence that foreign members are directing American children.

RESTRICTED - PROPRIETARY INFORMATION. The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBSCURA, LLC. RESTRICTED FROM DISCLOSURE // NOT FOR PUBLIC RELEASE OR NEWS MEDIA

TLP CLEAR – IN OBSCURA CAVEATS APPLY

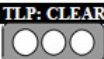
TLP CLEAR – DISSEMINATION UNLIMITED

///END///

=====

REQUEST WRITTEN PERMISSION, EMAIL, PRIOR TO DISSEMINATING ANY IN OBSCURA PRODUCTS OR INFORMATION. TRAFFIC LIGHT PROTOCOL REQUIREMENTS FOR DISSEMINATION

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
 TLP:RED For the eyes and ears of individual recipients only, no further disclosure.	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved.	Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.
 TLP:AMBER Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that TLP:AMBER+STRICT restricts sharing to the organization only.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.
 TLP:GREEN Limited disclosure, recipients can spread this within their community.	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.
 TLP: CLEAR Recipients can spread this to the world, there is no limit on disclosure.	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

///END OF REPORT///

RESTRICTED - PROPRIETARY INFORMATION. The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBSCURA, LLC. RESTRICTED FROM DISCLOSURE // NOT FOR PUBLIC RELEASE OR NEWS MEDIA

TLP CLEAR – IN OBSCURA CAVEATS APPLY