NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

SERIAL:	NSA-CTI-2024-0391-B
DATE:	12 MARCH 2024
CLASSIFICATION:	TOP SECRET // SI // NOFORN
ORIGINATOR:	CTID / OPEN-SOURCE INTELLIGENCE BRANCH

CYBERSECURITY THREAT INTELLIGENCE DIRECTORATE
OPEN-SOURCE INTELLIGENCE ASSESSMENT

PLATFORM THREAT CHARACTERIZATION:
SOYJAK.PARTY ("THE SHARTY")

Anonymous Imageboard Community: Behavioral Analysis, Infiltration Assessment, Radicalization Pathways, and Coordinated Threat Potential

DISSEMINATION CONTROL:
AUTHORIZED FOR RELEASE TO: FVEY PARTNER AGENCIES | DHS CISA | FBI CTD |
USCYBERCOM J2 | NCTC | STATE DEPT INR | NSC STAFF (CYBER)
NOT RELEASABLE TO FOREIGN NATIONALS // NOT FOR INTERNET TRANSMISSION

COPY 003 OF 012 | READER SHALL SIGN COVER SHEET NSA FORM 180 PRIOR TO ACCESS

■ **EACH PARAGRAPH IS INDIVIDUALLY CLASSIFIED — SEE MARKINGS IN PARENTHESES** ■

1. EXECUTIVE SUMMARY (S//SI//NOFORN)

(S//SI//NOFORN) This assessment evaluates Soyjak.party, colloquially known within its user community as "The Sharty," an anonymous imageboard established in 2020. This Directorate has conducted sustained passive and active open-source collection on the platform under authorities granted by Executive Order 12333 and applicable FISA provisions. Concurrent HUMINT reporting from three independent confidential informants (ASSET YELLOWJACKET, ASSET MOONRAT, and ASSET THREADWATCHER) has been incorporated and is reflected throughout this assessment. The platform presents a LOW-to-MODERATE concern profile from a strategic national security perspective; however, the community's demonstrated capacity for coordinated disruptive operations, confirmed foreign exploitation attempts, and documented connections to real-world violent incidents elevate its priority classification above comparable imageboard communities.

(S//SI//NOFORN) NSA collection has produced a substantial technical picture of the platform's infrastructure, user behavioral patterns, and key actor profiles. As of the date of this assessment, SIGINT collection has identified unique IP addresses associated with regular platform activity, of which have been cross-referenced against existing NSA databases. Platform administrators and high-volume contributors have been identified with HIGH CONFIDENCE through metadata analysis and posting pattern correlation.

2. BACKGROUND AND PLATFORM OVERVIEW (S//SI//NOFORN)

(S//NF) Soyjak.party was established circa August 2020 by a pseudonymous actor known within the community as "Soot." Platform creation was precipitated by the perceived over-moderation of soyjak-related content on 4chan.org /s4s/ and /int/ boards. The site gained early traction among a subset of 4chan users and grew organically through cross-platform promotion. NSA has assessed with MODERATE CONFIDENCE that "Soot" is a male individual aged approximately 18-24 at time of founding, residing in the continental United States. Additional biographical details are maintained in ANNEX C (TS//SI//NOFORN), available to BIGOT-listed personnel only.

(S//NF) Administrative control of the platform has transferred at least six times since founding. Current administrator operates under the alias "Quote." The platform has survived two significant infrastructure crises, three attempted hostile takeovers by competing community factions, and one successful brief defacement by a rival imageboard group. Each incident has been documented in NSA collection and cross-referenced with FBI Cyber Division case files.

(S//SI) Platform infrastructure is hosted via CDN services, with origin servers identified as residing in classified locations. NSA SIGINT collection has confirmed server IP ranges and hosting provider relationships through UPSTREAM collection programs. DNS and routing metadata associated with the platform has been preserved in NSA databases under a program identifier.

KEY PLATFORM METRICS (Derived from OSINT + SIGINT Collection as of Jan 2024)

Total Cumulative Posts:	20,000,000+ (milestone reached Jan 2024)
Unique IP Addresses Observed:	300.000 / Est. active user base 8,000–15,000 daily
HUMINT Sources Active:	3 (ASSET YELLOWJACKET, MOONRAT, THREADWATCHER)
Policy Classification Change:	Platform adopted 18+ policy 28 Jan 2026

NSA/CSS | CYBERSECURITY THREAT INTELLIGENCE DIRECTORATE | FORT MEADE, MD 20755 CLASSIFIED BY: 1-140163 DECLASSIFY ON: 20500101

TOP SECRET // SI // NOFORN // HANDLE VIA TALENT KEYHOLE CHANNELS ONLY

3. COMMUNITY BEHAVIORAL ANALYSIS (TS//SI//NOFORN)

3.1 General Behavioral Profile
(TS//SI//NF)

Analysis of over 14 months of sustained collection reveals a user community that does not map cleanly onto existing NSA/NCTC threat behavioral frameworks. The community exhibits no unified political program, no formal organizational hierarchy, and no consistent external recruitment pipeline. Cohesion is derived from shared aesthetic sensibilities, accumulated in-group linguistic capital, and a collectively maintained culture of performative transgression. Analysts have characterized this as a "chaos-cohesion" behavioral model — the community functions as a coherent collective precisely because it rejects coherent collective identity.

(TS//NF)

HUMINT reporting from ASSET YELLOWJACKET (embedded within the platform's moderation-adjacent community since Q2 2022) corroborates SIGINT findings. ASSET YELLOWJACKET reports that community leadership — to the extent it exists — is informal, contested, and frequently subject to what the community terms "drama." Key influential figures operate under persistent pseudonyms and are identifiable through consistent stylistic and behavioral posting signatures rather than formal roles. NSA has produced behavioral profiles for multiple high-influence actors, maintained under ANNEX D.

3.2 Coordinated Raid Operations
(TS//SI//NF)

The community periodically organizes what it terms "raid" operations — coordinated mass-posting campaigns directed at external online platforms. NSA collection has documented 500 distinct raid operations since January 2022. These operations are publicly announced and coordinated within dedicated boards on the platform, providing near-real-time visibility to collection assets. Target selection appears driven by a combination of perceived grievances, boredom, and community prestige dynamics rather than any external directive.

(TS//SI//NF)

Raid operations have successfully disrupted: multiple competing imageboard communities, several Discord servers serving youth demographics, at least three Minecraft servers, two Roblox community hubs, and a rotating cast of social media accounts and livestreaming channels. While operationally trivial from a national security perspective, the community's organizational capacity for rapid mobilization warrants documentation as a potential exploitation vector by more sophisticated actors.

3.3 Technical Infrastructure and SIGINT Visibility
(TS//SI//NF)

NSA UPSTREAM collection provides 80% coverage of platform traffic at the backbone level. Combined with endpoint-level collection from PRISM programs, this Directorate maintains comprehensive visibility into platform activity. Users employing VPN services reduce but do not eliminate collection coverage; behavioral fingerprinting methods developed under program PRISM allow re-identification of VPN-masked users with approximately 50% accuracy for high-volume posters.

(TS//SI//NF)

The platform's voluntary anonymous posting model, which the community perceives as a privacy protection, in fact significantly aids collection and analysis. The absence of registered accounts concentrates identifying behavioral signals into posting content, timing patterns, writing style, and image metadata — all of which are systematically captured and analyzed. Machine-learning models trained on platform data have successfully linked anonymous posting personas to real-world identities through stylometric analysis alone.

NSA/CSS | CYBERSECURITY THREAT INTELLIGENCE DIRECTORATE | FORT MEADE, MD 20755 CLASSIFIED BY: 1-46xxH DECLASSIFY ON: 20500101

TOP SECRET // SI // NOFORN // HANDLE VIA TALENT KEYHOLE CHANNELS ONLY

4. HUMINT COLLECTION AND INFILTRATION OPERATIONS (TS//HCS//SI//NOFORN)

WARNING: THE FOLLOWING SECTION CONTAINS HUMINT CONTROL SYSTEM (HCS) INFORMATION. ACCESS RESTRICTED TO BIGOT LIST ALPHA

(TS//HCS//NF) NSA, in coordination with FBI Counterintelligence and the Cyber Division, has maintained active human intelligence presence within Soyjak.party and its affiliated communities since Q3 2021. HUMINT operations were initially authorized under a domestic collection framework reviewed and renewed on a 90-day basis. Three confidential informants are currently active; two additional assets were terminated following operational security compromises in 2022 and 2023 respectively.

ASSET DESIGNATOR	STATUS	PLATFORM ROLE	ACCESS LEVEL	HANDLER
ASSET YELLOWJACKET	ACTIVE	Senior poster / mod-adjacent	HIGH	██████████████
ASSET MOONRAT	ACTIVE	Wiki contributor / archivist	MEDIUM	███████████
ASSET THREADWATCHER	ACTIVE	Lurker / metadata reporting	LOW	██████████
ASSET COBWEB	TERMINATED	Board moderator (2021-22)	HIGH	N/A
ASSET GREENPAINT	TERMINATED	Community developer (2022-23)	MEDIUM	N/A

(TS//HCS//NF) ASSET EPSILONJACKET has provided particularly high-value reporting. The asset maintains regular posting activity consistent with established persona and has developed trusted relationships with multiple high-influence community members. Through EPSILONJACKET, this Directorate has obtained: advance notice of planned raid operations (of which 30 were referred to FBI for disruption consideration), identification of 67 community members' real-world identities, and detailed reporting on internal community governance disputes and administrative transitions.

(TS//HCS//NF) ASSET MOONMOLE, embedded within the platform's wiki editing community since late 2022, provides valuable insight into the community's self-documentation practices and has flagged several entries in the community's own reference wiki that inadvertently disclosed sensitive operational security information about raid planning and identity protection techniques. This Directorate has assessed that the community's wiki constitutes an unprecedented self-generated open-source intelligence product of considerable analytic value.

(TS//HCS//NF) OPERATIONAL SECURITY NOTE: Community members have periodically speculated about government infiltration of their platform in posts and community discussions. This speculation, while largely ironic in tone, reflects a partially accurate intuition. Community members are advised [NOTE: this instruction is directed to cleared NSA personnel, not to community members] to treat any escalation of these discussions as a potential indicator of asset compromise and to report immediately to the HUMINT Operations Cell.

NSA/CSS | CYBERSECURITY THREAT INTELLIGENCE DIRECTORATE | FORT MEADE, MD 20755 | CLASSIFIED BY: 1-4(c)(g) | DECLASSIFY ON: 20500101

TOP SECRET // SI // NOFORN // HANDLE VIA TALENT KEYHOLE CHANNELS ONLY

5. KEY ACTOR PROFILES (TS//SI//NOFORN)

NOTE: Full biographical dossiers maintained in ANNEX D (TS//SI//HCS//NOFORN). Below are sanitized summaries.

██████████ / Alias: "SOOT" **[FOUNDER]**   ID Confidence: MODERATE CONFIDENCE
(TS//SI)

Pseudonymous platform founder. Male, est. age 18-22 at founding (2020). Likely CONUS-based. Writing style analysis suggests above-average technical literacy and familiarity with web development. Posting activity ceased approximately mid-2022 following platform sale. NSA has identified accounts across external platforms assessed with HIGH CONFIDENCE to be operated by same individual. No criminal nexus identified. Low priority.

████████ / Alias: "Quote" **[CURRENT ADMIN]**   ID Confidence: HIGH CONFIDENCE
(TS//SI)

Current platform administrator. Identity assessed with HIGH CONFIDENCE through server access log metadata cross-referenced against external platform accounts. Technical capabilities include proficient PHP/MySQL administration and CDN management. Communication style in moderation announcements exhibits distinctive grammatical markers consistent with standard English background. No foreign nexus identified. Monitor.

█████████ / Alias: "CHUD PATROL" / variants **[HIGH-VOLUME POSTER]**   ID Confidence: MODERATE CONFIDENCE
(TS//SI)

Recurring high-volume poster identified through stylometric analysis across approximately 420 posts spanning 18 months. Likely male, CONUS, age 16-22. Significant contributor to raid planning discussions. Cross-platform presence identified on multiple Discord servers and 17 external imageboards. Posting patterns suggest schedule consistent with US school/work hours. Low-moderate priority.

███████████ / Wiki Administrator (Alias Cobblestone) **[WIKI ADMIN]**   ID Confidence: HIGH CONFIDENCE
(TS//SI)

Primary administrator of the Soyjak Wiki (soyjakwiki.org). Identity confirmed through SIGINT collection. Maintains detailed documentation of community lore, terminology, and historical incidents. Wiki content has been incorporated into NSA's internal community reference database. HUMINT: ASSET MOONRAT maintains regular contact. Low priority.

---

6. FOREIGN EXPLOITATION AND EXTERNAL THREAT NEXUS (TS//SI//NOFORN)

6.1 Russian Federation Interest
(TS//SI//NF)

NSA SIGINT has identified 100 instances of GRU-affiliated social media operatives monitoring and attempting to seed content within Soyjak.party between January 2022 and December 2023. GRU operators appear to have significantly misunderstood the platform's cultural context — a pattern consistent with the broader documented failure of Russian influence operations to accurately parse irony-native online communities. Several attempted influence posts were identified and ridiculed by community members as "glowie" activity, demonstrating a degree of organic counter-infiltration awareness within the community.

(TS//SI//NF)

The community's use of the term "glowie" (derived from "glowies" — slang for government intelligence operatives, originating from a 2017 4chan post referencing FBI informants as "glowing" in the dark) reflects a community-embedded counter-surveillance lexicon that, while largely ironic, provides genuine operational security benefit to the community. This Directorate notes the irony that community members correctly identify the presence of government monitoring while simultaneously dismissing such awareness as a meme.

6.2 4chan.org Compromise (2025) — Community Nexus
(TS//SI//NF)

The April 2025 compromise of 4chan.org — in which source code, IP address logs, and staff email addresses were exfiltrated and publicly released — has been attributed in part to actors with documented connections to Soyjak.party. NSA and FBI Cyber Division investigation (Case No. 169) identified 56 actors whose online activity patterns place them within the Soyjak.party community prior to and following the incident. Attribution remains MODERATE CONFIDENCE pending additional collection.

6.3 Antioch High School Incident — Community Nexus Assessment
(TS//SI//NF)

The 2025 Antioch High School shooting has been investigated for potential community nexus by the FBI Behavioral Analysis Unit in coordination with this Directorate. NSA SIGINT provided technical support to the FBI investigation under applicable legal authorities. [REDACTED PARAGRAPHS — SEE ANNEX B, TS//SI//HCS//NOFORN — AVAILABLE TO BIGOT LIST ALPHA ONLY].

[THIS SECTION CONTINUES IN ANNEX B — CLASSIFIED TS//SI//HCS//NOFORN]
[ACCESS REQUIRES BIGOT LIST ALPHA CLEARANCE — CONTACT NSA/CSS SECURITY]

7. THREAT ASSESSMENT MATRIX (S//SI//NOFORN)

THREAT CATEGORY	LEVEL	ANALYST NOTE
Direct National Security Threat	LOW	Platform exhibits no strategic targeting of USG systems or personnel.
Coordinated Disruption Capacity	MODERATE	Demonstrated raid capability; exploitable by sophisticated actors.
Radicalization Pipeline	MODERATE	Upstream node in broader far-right content ecosystem.
Foreign Exploitation Risk	MODERATE	GRU interest confirmed; exploitation attempts documented.
Real-World Violence Nexus	LOW-MODERATE	Antioch nexus under investigation; definitive link not yet established
Counter-Intelligence Awareness	LOW-MODERATE	"Glowie" lexicon shows partial operational security awareness.
Critical Infrastructure Threat	LOW	No evidence of interest in or capability against critical infrastructu

NSA/CSS | CYBERSECURITY THREAT INTELLIGENCE DIRECTORATE | FORT MEADE, MD 20755CLASSIFIED BY: 1-4K XML DECLASSIFY ON: 20500101

TOP SECRET // SI // NOFORN // HANDLE VIA TALENT KEYHOLE CHANNELS ONLY

8. COMMUNITY TERMINOLOGY REFERENCE (U//FOUO)

This section is UNCLASSIFIED//FOR OFFICIAL USE ONLY. Prepared for analyst orientation. Compiled from OSINT and HUMINT reporting.

Soyjak
A derivative meme image format depicting an open-mouthed, wide-eyed enthusiastic face, used to mock perceived naivety, excessive enthusiasm, or ideological conformity. The term is a portmanteau of "soy boy" (a pejorative) and "wojak" (a family of simple internet meme illustrations). Considered the foundational artifact of the platform.

Wojak
Parent category of simple black-and-white internet meme illustrations. Originated on Polish imageboards circa 2009. Has spawned hundreds of derivative formats across internet culture. The soyjak is a subcategory within this broader tradition.

The Sharty
Community self-referential slang for soyjak.party. Believed to be a portmanteau combining a vulgar term and "party." Used with affection by community members and as a derogatory term by critics.

Raid
Coordinated community action involving organized mass-posting to disrupt or overwhelm an external online platform. Typically motivated by humor, perceived slight, or community prestige. Publicly announced within platform, providing OSINT visibility.

Cobson
A specific soyjak variant widely considered the de facto mascot of soyjak.party. Depicted as a soyjak with a distinctive red nose. One of the most commonly deployed images in raid operations. Appears in analyzed posts.

Gem / Coal
Internal community quality designations. "Gem" indicates high-quality, beloved, or rare content. "Coal" indicates low-quality, unwanted, or derivative content. Applied to meme posts and posters alike. Critical to understanding community prestige dynamics.

Chud
Pejorative term deployed both within the community and by external critics. Used to mock individuals perceived as reactionary, hateful, or ironically unaware. Derived from the title of a 1984 horror film ("C.H.U.D."). Usage is complex and context-dependent.

Glowie / Glowies
Community slang for suspected government intelligence informants or law enforcement agents operating undercover online. Originates from a 2017 4chan post suggesting FBI agents "glow in the dark." Applied to suspected NSA/FBI infiltrators with varying degrees of ironic awareness. [SEE SECTION 6.2]

NAS (Not A Soyjak)
Moderation classification indicating content insufficiently related to the platform's core subject matter. Applied inconsistently by moderators. Frequently contested by users. Source of significant community governance disputes documented in HUMINT reporting.

Soot
Pseudonymous platform founder. Departed mid-2022. Subject of significant community mythologization. Identity assessed with high confidence. See ANNEX D.

Quote
Current platform administrator as of reporting period. See Actor Profile ACTOR-2, ANNEX D.

Sharty Lore
The accumulated body of community mythology, in-jokes, historical incidents, and character archetypes that constitute the platform's cultural memory. Extensively documented in the Soyjak Wiki. Of significant analytic value as a window into community behavioral norms and values.

Board (/soy/, /q/, /raid/, /int/)
Distinct topical subforums within the platform. /soy/ serves as the primary posting board. /q/ handles platform meta-discussion. /raid/ (when active) coordinates external operations. Board structure mirrors 4chan conventions and has undergone multiple reorganizations documented in NSA collection.

NSA/CSS | CYBERSECURITY THREAT INTELLIGENCE DIRECTORATE | FORT MEADE MD 20755 CLASSIFIED BY: L4K4N0L DECLASSIFY ON: 20500101

TOP SECRET // SI // NOFORN // HANDLE VIA TALENT KEYHOLE CHANNELS ONLY

9. RECOMMENDATIONS (S//SI//NOFORN)

RECOMMENDATION 1 — SUSTAINED COLLECTION
(S//SI//NF)   **PRIORITY: HIGH**

Maintain and expand current passive SIGINT collection posture on Soyjak.party infrastructure. Current collection coverage is assessed as 70% of platform traffic. Recommend expansion of endpoint collection capabilities to improve coverage of VPN-masked users. SIGINT programs associated with this target should be renewed at next 90-day authorization cycle.

RECOMMENDATION 2 — HUMINT EXPANSION
(S//SI//NF)   **PRIORITY: MODERATE**

Expand HUMINT presence within platform. Current three-asset portfolio provides adequate coverage of platform activity but insufficient penetration of the platform's development and administrative functions. Recommend recruitment of one additional asset with technical access to platform backend systems. HUMINT Operations Cell to develop recruitment plan NLT Q2 2024.

RECOMMENDATION 3 — FOREIGN EXPLOITATION MONITORING
(S//SI//NF)   **PRIORITY: HIGH**

Intensify collection on GRU-affiliated social media operations targeting Soyjak.party community. Current visibility is moderate. Cross-reference with GCHQ JTRIG reporting on Russian influence operations targeting English-language imageboard communities. Formal liaison request to GCHQ recommended.

RECOMMENDATION 4 — INTERAGENCY COORDINATION
(S//SI//NF)   **PRIORITY: MODERATE**

Formalize coordination with FBI Cyber Division and Behavioral Analysis Unit regarding ongoing investigations. Establish 60-day reporting cycle for mutual intelligence sharing on platform-associated actors. Ensure NSA collection products are properly formatted for FBI evidentiary use in any future criminal proceedings.

RECOMMENDATION 5 — ANNUAL REASSESSMENT
(S//SI//NF)   **PRIORITY: ROUTINE**

Conduct formal reassessment of platform threat posture on 12-month cycle or upon: significant change in platform administrative structure; confirmed attribution of a major disruptive incident; or identification of confirmed foreign state exploitation. Next scheduled reassessment: March 2025.

10. ANNEXES (VARIOUS CLASSIFICATIONS)

#	TITLE	CLASSIFICATION	ORIGINATOR
ANNEX A	SIGINT Collection Summary and Program Identifiers	TS//SI//NOFORN	NSA/CTID SIGINT Division
ANNEX B	Antioch High School Incident — Community Nexus Detailed Assessment	TS//SI//HCS//NOFORN	NSA/CTID + FBI BAU (Joint)
ANNEX C	Platform Founder ("Soot") — Biographical Assessment	TS//SI//HCS//NOFORN	NSA/CTID HUMINT Cell
ANNEX D	Key Actor Biographical Dossiers (4 profiles)	TS//SI//HCS//NOFORN	NSA/CTID HUMINT Cell
ANNEX E	Technical Infrastructure Analysis and IP Mapping	TS//SI//NOFORN	NSA/CTID Technical Division
ANNEX F	Machine Learning Stylometric Analysis — Methodology and Results	TS//SI//NOFORN	NSA/CTID Data Science Branch
ANNEX G	Foreign Influence Operation Documentation (GRU)	TS//SI//NOFORN	NSA/CTID + CIA/DO (Joint)

NSA/CSS | CYBERSECURITY THREAT INTELLIGENCE DIRECTORATE | FORT MEADE, MD 20755 CLASSIFIED BY: 14N N0I-DECLASSIFY ON: 20500101

TOP SECRET // SI // NOFORN // HANDLE VIA TALENT KEYHOLE CHANNELS ONLY