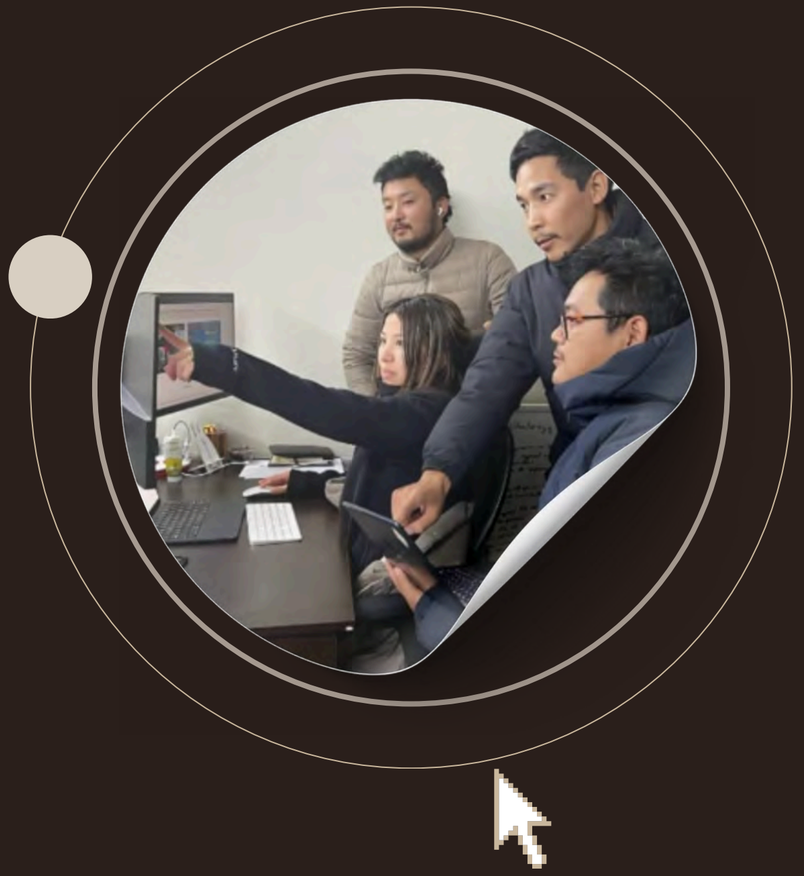
A CASE FOR THE DNS SECURITY COMMUNITY

Cyber Threats Against the Tibetan Diaspora



Twenty years of DNS abuse, email abuse, targeted malware, and infrastructure attacks — Can an at-risk community collaborate with ICANN & SSAC ?

Robert Guerra Privaterra · ICANN SSAC · Toronto
Tenzin Gyal Program Manager, Tibet Action Institute / TibCERT · Dharamsala

Why this talk, why SSAC

Three points before we start.

01 A security briefing, not an advocacy talk

The next 15 minutes use one well-documented target community as a lens for DNS abuse, email abuse, targeted malware, and infrastructure attacks.

02 Issues within SSAC’s remit

Lookalike domains, registrar abuse, mail-flow compromise, root-zone / IDN questions, watering-hole CMS attacks, and as of 2025, cellular-layer SS7/DIAMETER tradecraft. All technically receipt-checked.

03 A concrete closing ask

Four ways an SSAC member, a registrar, registry, hosting provider, or ICANN 86 participant can help. Not just "raising awareness", but asking for specific opportunities for collaboration.

The community at a glance

Small, well-documented, under-resourced

~100,000

Tibetans in exile worldwide

50+

organizations in the TibCERT coalition

20+ years

of continuous, attributed cyber targeting

1 hub

Dharamsala · ~~Dehradun~~ · ~~Bylakuppe~~ · ~~Mundgod~~

Dharamsala, Himachal Pradesh — seat of the Central Tibetan Administration

Mundgod Tibetan Settlement, Karnataka, India — Volunteers from Response Hub distributing pamphlets and other digital security resources on World Password Day.

A glimpse of Tibetan Women's Association (TWA) receiving annual digital security policy review sessions.

A debate session on "The Impact of Social Media in the Tibetan Community."

Source: TibCERT, TAI Digital Security

From the first connection to a coalition CERT

How the Tibetan diaspora went from "first computer in Dharamsala" to running a real CERT — because the attacks never stopped.

1997	**Internet arrives in Dharamsala** Dan Haig and team bring the first connection to the Central Tibetan Administration (then the Tibetan Government in Exile).
1999–2001	**First spoofed-email attacks** An unnamed virus posing as mail from the Dalai Lama's office targets Tibet lobby groups; Chinese actors attempt direct intrusions.
2009	**GhostNet exposed** Citizen Lab and Information Warfare Monitor map the network compromising OHHDL, CTA, and diaspora NGOs.
2010	**Shadows in the Clouds** IWM and Shadowserver document a second network exfiltrating sensitive data from the same offices.
2011–2014	**TAI digital security campaigns** "Detach from Attachments," "HTTPS Keeps Your Secrets Safe," "Don't Share Drives," "Keep Your Enemy Out of Your Inbox."
2012–2017	**APT TA413 / LuckyCat** Relentless targeting via computer and mobile malware, website infections, and browser-based phishing.
2017+	**Mobile-first pivot** Compromised versions of legitimate Android apps replace email attachments as the primary delivery vector.
2018	**TibCERT founded** Coalition-based Computer Emergency Readiness Team under TAI — prevention and mitigation, by and for the community.
2018–2019	**POISON CARP** One-click WhatsApp exploits hit senior figures via seven fake personas — journalists, advocates, tourists.

Dharamsala — home of the Central Tibetan Administration, the Office of the Dalai Lama, and TibCERT.

Source: TibCERT — Threat & Target, Citizen Lab GhostNet, Shadows in the Clouds

Twenty years on the front line

Every major civil-society APT story of the last fifteen years either started here, or arrived here within months.

First public proof: APT-grade infrastructure aimed at civil society.

Mobile escalation begins.

Beyond DNS: the cellular layer.

2009

GhostNet

1,295 hosts, 103 countries; OHHDL, ICT compromised.

2012

Self-immolation IO

CVE-2010-3333 RTF lures, RTLO Unicode tricks.

2014

Communities @ Risk

TAI + 9 CSOs face the same APTs as governments.

2018-19

POISON CARP

1-click WhatsApp exploits; 17 high-profile targets.

2021

TA413 / FriarFox

Malicious Firefox extension reading Gmail.

2024

GhostChat / PhantomPrayers

Dalai Lama 90th birthday lures via niccenter[.]net.

2025

SS7 / Lhasa centre

Cellular-layer attack; new offensive-cyber facility.

Source: Citizen Lab GhostNet, Citizen Lab POISON CARP, TibCERT 2024

Tibet Action Institute

Digital communication tools + strategic nonviolent action. Founded 2009.

FOUNDERS

Lhadon Tethong · Nathan Freitas (Guardian Project)

DIRECTOR OF TECHNOLOGY

Lobsang Gyatso Sither — Frequent USCIRF testifier, Parliamentarian

FLAGSHIP PROGRAMS

TibCERT · Digital Security Ambassadors · Research and Reporting

RECENT REPORTS (2024)

Digital Disruption · Cyber Espionage Against Tibetans

RECOGNITION

2019, 2024 NED Democracy Award · 2024 Snow Lion Prize (Tethong)

Source: tibetaction.net, TAI Wikipedia, Sither USCIRF testimony

TibCERT — a real CERT, for an at-risk community

Tibetan Computer Emergency Readiness Team. A TAI program since 2018.

1. RESEARCH

Evidence-based research to understand threats and inform stronger solutions.

- Publish reports with security and research partners
- On-field, evidence-based research works
- Threat landscape and incident analysis
- Documentation of cyber incidents and case studies
- Policy-oriented research and recommendations

2. TIBCERT INFRASTRUCTURE

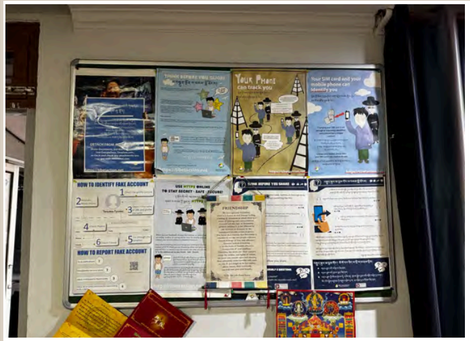
Building and maintaining secure systems to detect, respond and protect.

- HelpDesk and Incident Response Support
- Wazuh Endpoint Detection and Monitoring
- IDS Deployments and Network Monitoring
- Mobile Forensics – PiRogue Analysis
- Security Tools Deployment and Management

3. DIGITAL SECURITY TRAINING

Empowering individuals and organizations with skills and policies for digital safety.

- Capacity Building Trainings
- Digital Security Policy Development and Review
- Cyber Hygiene and Awareness Workshops
- Secure Communications Training
- Training for NGOs, Journalists, Researchers & Communities
- Social Media Safety and Account Protection



TAI "Stay Safe Online" posters · Dharamsala

Community Awareness Program · South India

Digital Security Training · Dharamsala

Reviewing Digital Security Policy · Dharamsala

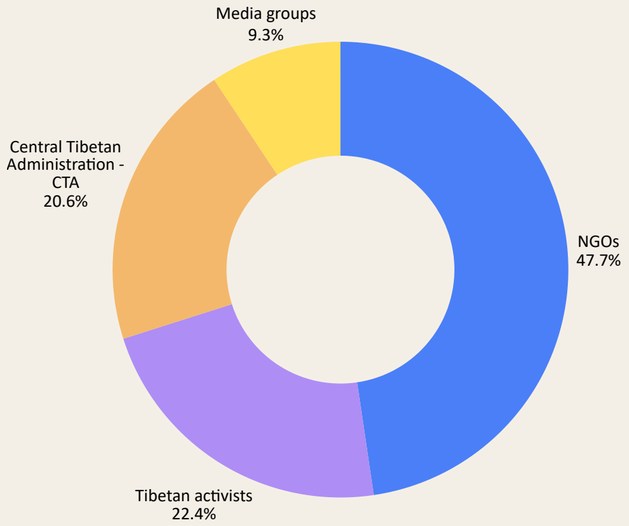
50+ member organizations · **1 hub** Dharamsala · ~~Dehradun · Bylakuppe · Mundgod~~

Source: tibcert.org, TAI Digital Security

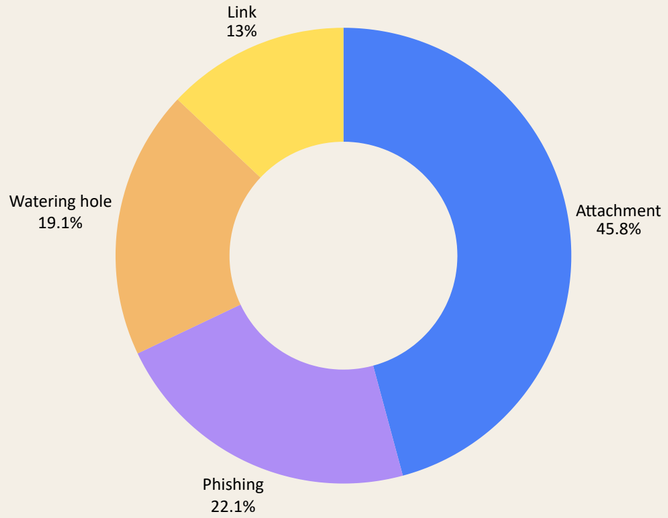
TibCERT 2026 — two decades, structured

Publishable, replicable, technical telemetry from a civil-society CERT.

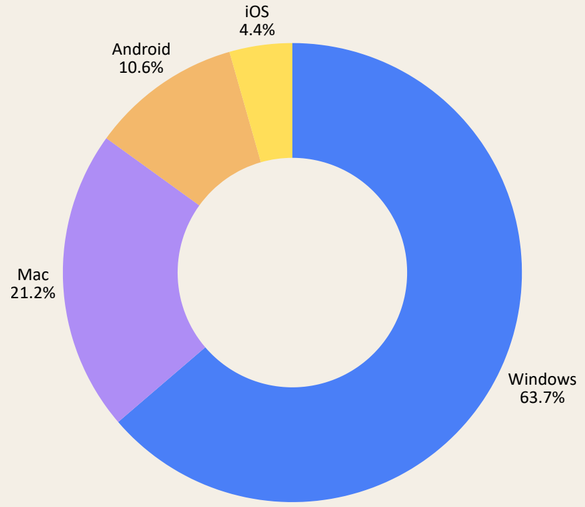
MOST-TARGETED VICTIMS



DOMINANT INCIDENT VECTORS



PLATFORM DISTRIBUTION



Citizen Lab finding: simply not opening unsolicited email attachments would have prevented over 95% of malware reaching Tibetan groups in the early 2010s.

Source: TibCERT 2024 — Cyber Espionage Against Tibetans, Digital Disruption

IDN & Universal Acceptance — the Tibetan-script gap

Simultaneously a homoglyph-defense gap and an inclusion gap. ICANN-community work by definition.

DEFENSIVE

Lookalike & homoglyph domains

Tibetan-script publishing is rare; the diaspora hosts in English and romanized Tibetan. That makes the entire impersonation playbook easier — and the registrar-abuse playbook richer.

OBSERVED IN 2025

`icjiorg[.]org`
`epechtimes0[.]org`
`epochtimes.entryfortify[.]com`

INCLUSIVE

Tibetan script & Universal Acceptance

Tibetan script (Unicode U+0F00–U+0FFF) is not delegated as an IDN root-zone label generation rule. UA of Tibetan-script domains and email is an open ICANN policy question.

OPEN ICANN WORKSTREAMS

- Root Zone LGR for Tibetan-script
- UA of IDN email at registrars and at MUAs
- Engagement with Tibetan-language community

Source: ICANN Universal Acceptance, IDNs at ICANN, Citizen Lab — Tall Tales

DNS & registrar abuse — the entry point

Legitimate providers, abused at scale. Standing SSAC interest in registrar abuse-response practice.

REGISTRATIONS

Lookalike & typosquat domains

- **Registrars** - Commonly used by bad actors globally

`niccenter[.]net` and subdomains delivered Gh0st RAT and PhantomNet during the Dalai Lama 90th-birthday lures (GhostChat / PhantomPrayers, 2024).

HOSTING

IPs serving phishing kits

- **Hosting Providers** - with weak abuse response

Persistent diaspora-targeting kits hosted on small HK and APAC infrastructure providers — same IP ranges across campaigns.

Used in GhostChat/PhantomPrayers attacks targeting the Dalai Lama

SENDING

Mail-flow abuse

- smtp.secureserver[.]net (**GoDaddy Workspace**)
- **AWS S3** to host malicious HTML

Legitimate **sending infrastructure r**epeatedly used by Chinese-actor clusters — including for sender impersonation of OHHDL and TWA.

Source: Citizen Lab — Tall Tales, Cybernews / Zscaler ThreatLabz

Email abuse — the dominant vector

Tighten deployment of DMARC, DKIM, SPF by targeted organizations

> 90%

of cyber attacks on the Central Tibetan Administration (CTA) begin with a phishing email.

— The Cyber War Against Tibet, CTA

THEMED LURES OBSERVED

March 10	Tibetan National Uprising Day anniversary
Dalai Lama Birthday	July 6 — annual campaigns; 2025 was a 90th-birthday peak
Kalachakra teachings	WeChat keyword censorship + spear-phishing
COVID / Delek Hospital	Sepulcher malware in PowerPoint (TA413, 2020)
Tibetan Women's Association	Sender impersonation + FriarFox Firefox extension (TA413, 2021)
Mailing-list compromise	"Tibet was never a part of China" PowerPoint → ExileRAT

Source: The Cyber War Against Tibet, CTA, Infosecurity — FriarFox, TibCERT 2024

Targeted malware — the long tail

Same tooling that hits governments. A tenth of the budget to defend against it.

DESKTOP RATs & BACKDOORS

GhostNet · Sepulcher · LOWZERO · Nightdoor · MgBot · Scanbox · ExileRAT · Gh0st RAT · PhantomNet

CVE-2012-0158, CVE-2010-3333, Lady Boyle SWF, Cobalt Strike, "Follina" CVE-2022-30190, Sophos CVE-2022-1040.

MOBILE

POISON CARP iOS 1-click (iOS 11.0–11.4) · MOONSHINE Android exploit kit · KakaoTalk & TuneIn fake APKs

WhatsApp-delivered links targeted 17 high-profile members including OHHDL and CTA staff (2018-2019).

ATTRIBUTED CLUSTERS

GhostNet · APT1 (Unit 61398) · POISON CARP · TA413 · EvilBamboo (Evil Eye) · Evasive Panda (TAG-102) · TAG-112

Drawn from Citizen Lab, Cisco Talos, Proofpoint, Volexity, Recorded Future, Zscaler, and TibCERT.

Source: TibCERT 2024, POISON CARP

Infrastructure attacks — beyond DNS

DDoS, watering-hole, CMS compromise — and as of 2025, the cellular layer.

DDoS

Sustained availability attacks

OHHDL, CTA, Voice of Tibet (combined with radio signal jamming, 2011), Tibetan NGOs in Dharamsala.

WATERING-HOLE & CMS

Trusted-site compromise

tibettimes.net, OHHDL website, CTA website, Tibetan Homes Foundation — Joomla CMS implants, malicious JS, fake Flash / certificate updates.

EDGE EXPLOITS

Firewall & document zero-days

CVE-2022-1040 (Sophos Firewall), "Follina" CVE-2022-30190 in document lures — exploited in the wild against Tibetan orgs.

CELLULAR LAYER (2025)

SS7 / DIAMETER / IMSI catcher

TibCERT documents zero-interaction location tracking of a senior Tibetan leader in exile — "Welcome to China" roaming messages received in India.

Source: TibCERT / Tibet Express SS7 advisory, TibCERT — Digital Disruption

What's new in 2026 — three signals

Each item is a concrete data point — not a trend story.

A

Operations GhostChat & PhantomPrayers

Dalai Lama 90th-birthday lures via a cloned Tibetan charity site under `niccenter[.]net`. Multi-stage Gh0st RAT and PhantomNet delivery. Watering-hole + culturally themed apps.

B

First publicly documented cellular-layer attack

TibCERT advisory: SS7 / DIAMETER / IMSI-catcher / IPX-operator manipulation against a senior Tibetan leader. Zero device interaction. Followed Dalai Lama "Voice for the Voiceless" book release (Mar 2025).

C

New Lhasa offensive-cyber facility

Offensive-cyber training + digital forensics lab at the Tibet Police College, built by US-Entity-listed Meiya Pico. ASEAN expansion via Vietnam. UK NCSC advisory Apr 9, 2025.

Year of Compassion — Dalai Lama 90th-birthday campaign was the lure theme for 2025 operations.

Source: Cybernews / Zscaler, TibCERT SS7 advisory, Tibetan Review — Lhasa cyber ops centre

The ICANN community is already helping

A worked example — contacts made inside this room, turned into operational protection for TAI and TibCERT.

IDN EXPERTISE

Tibetan-script IDN & UA scoping

SSAC members Jim Galvin and Nabil Benamar, with ICANN staff — helping scope what a Tibetan-script root-zone LGR and Universal Acceptance roadmap could look like.

CLOUDFLARE PROJECT GALILEO

tibetaction.net approved (early 2026)

Cloudflare onboarded TAI to free DDoS / WAF protection. Direct response to the diaspora-targeting threat profile we just walked through.

PROTON FOUNDATION

TibCERT nonprofit email application

Application underway for Proton Mail / Drive nonprofit access — sensitive comms for an at-risk-community CERT moving off general-purpose email.

i2COALITION

Hosting & security peers

i2Coalition member providers — connecting TAI to trusted hosting, registrar, and security operators inside the Internet Infrastructure Coalition.

Source: Cloudflare Project Galileo, Proton Foundation, i2Coalition

Four concrete asks

How an SSAC member, a registrar, a registry, or hosting provider can help

01 **Support & recognize civil-society CERTs as peers**

Support TibCERT — and similar at-risk-community CERTs (CiviCERT, Access Now) — so they can bring their knowledge, tactics, and research findings related to DNS abuse, security and stability discussions. ***See them as partners, and not just data sources.***

02 **Registrar/registry brief on diaspora-targeting domain abuse**

Focused write-up of the Tibet/Uyghur/Hong-Kong diaspora playbook — TLDs, naming patterns, registrant fingerprints, takedown SLAs encountered by victims.

03 **Tibetan-script IDN & Universal Acceptance**

Engage the Tibetan-language community on root-zone LGR work and the UA roadmap. Closes a homoglyph-defense gap and an inclusion gap at the same time.

04 **Email-authentication advisory for at-risk diasporas**

Community advisory on DMARC / DKIM / SPF deployment for at-risk-community email infrastructure. > 90% of CTA-targeted attacks start with email — measurable mitigation.

"The Tibetan diaspora has been doing research, handling DNS Abuse & security training for twenty years.

The technical community should not just read our reports — but let TibCERT “into the room."

Thank you.

Robert Guerra (Privaterra · ICANN SSAC) · Tenzin Gyal (TAI / TibCERT · Dharamsala)

Resources & further reading

Live links — stays on screen for Q&A.

- ICANN Universal Acceptance
- TibCERT
- Tibet Action Institute
- TAI Digital Security
- The Cyber War Against Tibet (CTA)
- Cloudflare Project Galileo
- Proton Foundation
- i2Coalition
- TibCERT 2024 — Cyber Espionage Against Tibetans
- TibCERT 2024 — Digital Disruption
- Citizen Lab — Tracking GhostNet: Investigating a Cyber Espionage Network (2009)
- Citizen Lab — POISON CARP
- Citizen Lab — Tall Tales (impersonation)
- TibCERT SS7 advisory (2025)
- Lobsang G. Sither — USCIRF testimony
- Targeted Attacks in the Tibetan Community

Thank you.

For your time, your questions, and the work the ICANN community already does for at-risk communities.

STAY IN TOUCH

Robert Guerra

CEO, Privaterra · ICANN SSAC

Toronto, Canada

rguerra@privaterra.org robert.19 (Signal)

privaterra.org

Tenzin Gyal

Program Manager, Tibet Action Institute / TibCERT

Dharamsala, India

tgyal@tibetaction.net tintin.213 (Signal)

tibetaction.net · tibcert.org

Questions, follow-ups, intros to TibCERT / TAI — all welcome.