NCA-24.050825 – National CERT Advisory – Responsible Use of Social Media Amid Escalations on the Eastern Border

Introduction

Amid the ongoing security escalations and intensified military activity along Pakistan's Eastern Border, the National Cyber Emergency Response Team (National CERT) issues this urgent advisory to media organizations, independent digital content creators, online influencers, and the general public.

This advisory underscores the imperative of exercising extreme discretion, vigilance, and digital responsibility during this volatile period. The unrestricted dissemination of media—photos, videos, or textual reports—revealing troop movements, operational details, or strategic deployments via social media can gravely undermine national security, endanger lives, and serve as a force multiplier for adversarial reconnaissance and propaganda efforts.

The public is strongly urged to prioritize operational security and national interest above personal visibility or engagement metrics on digital platforms.

Impact

Inappropriate or unauthorized sharing of sensitive content on social media can result in:

1. **Operational Security Breaches** – Live or time-stamped content exposing troop positions or movement paths can compromise tactical advantage.
2. **Adversarial Intelligence Gathering** – Open-source material posted online is often aggregated to form actionable insights against national interests.
3. **Geospatial Risk Amplification** – Geo-tagged or location-linked imagery may unintentionally map sensitive zones or infrastructure.
4. **Information Warfare Escalation** – Circulation of fake or manipulated content can destabilize public morale and trust.
5. **Legal Consequences** – Sharing classified, restricted, or misleading content may invite legal action under national security laws.
6. **Diplomatic Fallout** – Misinformation may provoke unintended international reactions, straining diplomatic ties.

Threat Details

Key vectors of concern include:

1. **Unauthorized Content Dissemination**: Real-time uploads of military activity, logistics operations, or border troop deployments.

2. **Synthetic Media & Deepfakes**: AI-generated imagery or audio simulating events or statements to distort public perception.
3. **Viral Misinformation**: Rapid spread of misinterpreted or unverified claims about battlefield outcomes or incidents.
4. **Psychological Manipulation**: Attempts to provoke panic or unrest by exploiting public sentiment via digital narratives.

Affected Groups

- National and regional news outlets, both print and electronic.
- Freelance journalists and field correspondents.
- YouTube creators, bloggers, and social media influencers.
- General public, especially those in proximity to sensitive zones.
- Tech platforms and moderators of social communities.

Recommendations and Best Practices

1. **Content Restriction & Security**
    a. Refrain from filming or sharing any military convoys, troop deployments, or conflict-zone activity.
    b. Disable location sharing when capturing content in sensitive areas.
    c. Seek clearance before reporting or publishing on military-related developments.
    d. Blur insignias, faces, vehicle numbers, or tactical overlays in unavoidable visual content.
2. **Counter-Synthetic Media Practices**
    a. Scrutinize dramatic or sensational media; verify with multiple credible sources.
    b. Use reverse-image search and deepfake detection tools before reposting viral content.
    c. Be aware of visual inconsistencies: unnatural movements, mismatched audio, or abrupt frame cuts.
3. **Journalistic Integrity and Verification**
    a. Apply multi-layered editorial oversight on defense and conflict coverage.
    b. Clearly label all unverified claims or amateur footage as “Unconfirmed.”
    c. Cite official or authorized sources; avoid amplifying anonymous or speculative content.
    d. Prioritize national interest over engagement-driven reporting.
4. **Responsible Social Media Conduct**
    a. Do not repost or engage with unverified reports about border incidents or military actions.
    b. Report suspected fake content or sensitive disclosures to platform moderators or local authorities.

c. Follow official government channels for accurate, timely updates.
d. Discourage group-based speculation or “open-source intelligence” collection on social platforms.

5. **Legal Compliance**

a. Understand and respect national laws governing wartime reporting, defense coverage, and classified information.
b. Know that breaching operational confidentiality is a punishable offense.
c. Ensure all field correspondents and freelancers are briefed on content boundaries and legal liabilities.

6. **Strategic Protective Measures**

a. Encourage the use of digital watermarks and metadata validation for official media.
b. Collaborate with cybersecurity agencies to detect and neutralize synthetic content.
c. Work closely with social media companies to flag and takedown malicious or harmful media swiftly.
d. Maintain internal escalation protocols for countering misinformation and managing reputational risks.

7. **Public Awareness and Engagement**

a. Launch broad digital literacy campaigns to educate the public on risks of oversharing.
b. Distribute infographics, do’s and don’ts, and advisory posters across digital and physical platforms.
c. Host seminars/webinars for journalists and influencers on information warfare and synthetic media threats.
d. Promote a civic culture of cautious, verified, and patriotic digital communication.

Call to Action

National CERT strongly advises all digital participants to:

- Immediately refrain from recording, posting, or forwarding any content depicting military activity,
- Exercise strict caution against manipulated media or unverified rumors,
- Rely only on official sources for updates, and
- Uphold a digital ethic of responsibility, confidentiality, and national unity.

Every post counts. Every share matters. Let’s protect our armed forces, safeguard our national interests, and act as responsible citizens in these critical times.