CRONet Raspberry Pi Emergency Deployment Manual

Overview

This guide describes how to deploy the CRONet emergency communication system on a Raspberry Pi using a custom pseudo-TLD (.carrot). It is designed for field use in crisis zones where secure communication with the U.S. government is critical.

Setup Instructions

1. Flash Raspberry Pi OS Lite to a microSD card.
2. Boot and configure network (Ethernet/WiFi).
3. Copy 'bootstrap.sh', 'whistleblower_dropbox.py', and 'dod_public_key.asc' to the Pi.
4. Run the script:
   chmod +x bootstrap.sh && ./bootstrap.sh
5. Access the secure form at: http://relay1.carrot:8002/submit

Security Notes

- Only use on trusted, hardened networks.
- Ensure dod_public_key.asc is valid.
- Files are stored temporarily and encrypted.
- DNS is overridden locally for .carrot pseudo-TLD use.
- Use HTTPS tunneling or airgapped environments if possible.