OGRE ARMAGEDDON – Consolidated Blueprint (Agent ↔ HQ, LCARS/Borg, Section 31)

Updated: 2025-08-22

# 1) Architecture Overview

Portable \*\*Agent Node\*\* (USB/Pi) phones home to \*\*Ogre HQ (Jarvis Core)\*\* over WireGuard.  
Edge runs lightweight scans and interfaces; HQ handles AI, storage, and orchestration.  
Modes (Regular / Section 31 / Borg / Scorched Earth) control visuals and behavior.

# Agent Node – Local Modules

* ONVIF/RTSP discovery + selective brute-force (rate-limited)
* Evil Twin Wi‑Fi module (lab-only, disabled by default)
* USB‑to‑TTL serial bridge + optional firmware flashing
* Health pings + remote command channel (Socket.IO or MQTT)
* Minimal web/CLI; main dashboards live at HQ

# HQ – Central Services

* Jarvis AI Brain (GPT‑5 orchestrator + Codex for code + Sora/vision)
* Starfleet LCARS + Borg overlays + Section 31 covert theme
* RTSP ingest/decoding, analytics, and storage
* Multi‑node control, enrollment, RBAC, and audit logging

# 2) Storage Layout (Multi‑Disk)

# Mounts & Purpose

* 80 GB SSD → `/` (root; OS only)
* 128 GB SSD → `/ai` (models, caches, engines)
* 1 TB → `/srv` (logs, backups, artifacts, WG keys with strict perms)
* 1 TB (future) → `/ha` (video capture/monitoring ingest)

fstab example (use real UUIDs):

UUID=<ROOT-UUID> / ext4 defaults,noatime,errors=remount-ro 0 1  
UUID=<AI-UUID> /ai ext4 defaults,noatime 0 2  
UUID=<SRV-UUID> /srv xfs noatime,attr2,inode64,logbufs=8 0 2  
UUID=<HA-UUID> /ha xfs noatime,attr2,inode64,logbufs=8 0 2

# Best Practices

* Keep `/srv` and `/ha` separate to protect `/` from floods
* Enable SMART monitoring + email alerts; aggressive logrotate
* Consider `nodev,nosuid,noexec` on `/srv` if feasible

# 3) Modes & Visuals (LCARS/Borg/Section 31)

# Modes

* Regular: safe defaults, minimal noise
* Section 31: covert visuals, stealth tools (MAC spoofing, jittered scans, proxy hopping)
* Borg Assimilation: aggressive guidance and overlays
* Scorched Earth: maximum automation/power; launch codes + self‑destruct logging

# UI/UX

* LCARS panels (clean), Borg overlays (tactical), Section 31 black/red variant
* Sound FX toggle (default ON), accessibility: high‑contrast and reduced‑motion modes
* Real‑time panels: logs, RTSP previews, AI panel, node status

# 4) Security & Compliance

# Core

* WireGuard per‑node keys; rotation schedule; device NodeID and labels
* AppArmor/SELinux confinement for scanners, Wi‑Fi tools, ffmpeg, serial bridge
* Read‑only root for agents (overlayfs) + signed/immutable updates (optional)
* Central secrets management (sops/age or Vault); no secrets in images
* RBAC (admin/op/viewer) with OIDC/SSO if available
* Audit trail: command provenance, mode toggles, and changes logged

# Ethics/Policy

* Evil Twin and brute‑force modules \*\*lab‑only with written authorization\*\*
* Kill‑switch: global disable for offensive modules from HQ
* Rate‑limits and safeties to avoid target lockouts or DoS

# 5) Enrollment & Node Management

# Process

* On first boot, Agent generates keypair, sends enrollment request via bootstrap channel
* HQ approves → issues NodeID, labels, and policy set (mode defaults, limits)
* Node heartbeat shows health, versions, connected interfaces

# Ops

* Fleet view: list/search nodes; per‑node actions (restart services, rotate keys)
* Policy bundles per mode; staged rollouts; remote updates

# 6) Roadmap / Phases

# Phase 0 – Host & Disks

* Partition + mkfs; mountpoints; fstab; SMART + alerts; SSH keys; ufw/fail2ban

# Phase 1 – Ogre HQ

* Docker+compose, Jarvis Core + local LLM, Starfleet/Borg UI
* WireGuard server; enrollment flow; central logging (Loki/Promtail or Elastic)

# Phase 2 – Agent Image

* Minimal OS with scanner/Wi‑Fi/serial tools; WG client autostart
* Health pings; remote command channel (Socket.IO/MQTT)

# Phase 3 – Modes

* Implement mode toggles and policy bundles; visuals, sound FX

# Phase 4 – Video/Stream

* HQ RTSP ingest (ffmpeg/rtsp-simple-server); `/ha` retention and watchdogs

# Phase 5 – Hardening & Backups

* Secrets vault, automated backups, key rotation cadence and revocation CI

# Phase 6 – HA & Extras

* Read‑only agents; immutable updates; HQ HA pair (keepalived)

# 7) Ogre‑Bridge Pi — Design & Build

# Purpose & Roles

* Field bridge: lightweight scanner, Wi‑Fi lab, serial bridge; all heavy AI at HQ
* Auto‑WireGuard to HQ; no WAN‑exposed services

# Services on Pi

* ogre‑agent (Python): health, enrollment, telemetry, remote exec
* wg‑quick@wg0 (client)
* scanner (ONVIF/RTSP), rtsp‑probe (ffmpeg)
* wifi‑lab (disabled by default)
* serial‑bridge (USB‑TTL)

# Build Checklist

* Flash Raspberry Pi OS Lite; enable SSH; set hostname (ogre-bridge‑##)
* Install: wireguard, python3‑pip, ffmpeg, tcpdump, apparmor-utils
* Place wg0.conf; enable wg‑quick@wg0; install ogre‑agent + services
* Enroll node: pubkey allowlist at HQ; verify heartbeat and tunnel

# 8) WireGuard Templates (HQ / Agent)

HQ `/etc/wireguard/wg0.conf` (example):

[Interface]  
Address = 10.31.0.1/24  
ListenPort = 51820  
PrivateKey = <HQ\_PRIVATE\_KEY>  
SaveConfig = true  
  
# Example peer; repeat per agent  
[Peer]  
PublicKey = <AGENT\_PUBLIC\_KEY>  
AllowedIPs = 10.31.0.10/32  
# Optionally restrict to keep tunnel clean

Agent `/etc/wireguard/wg0.conf` (example):

[Interface]  
Address = 10.31.0.10/32  
PrivateKey = <AGENT\_PRIVATE\_KEY>  
DNS = 1.1.1.1  
  
[Peer]  
PublicKey = <HQ\_PUBLIC\_KEY>  
Endpoint = <HQ\_PUBLIC\_IP>:51820  
AllowedIPs = 10.31.0.0/24  
PersistentKeepalive = 25

# 9) Operational Safeties & Killswitches

# Safeties

* Global HQ kill‑switch for offensive modules (Evil Twin, brute)
* Per‑node rate limits and time windows; lockout detection
* Emergency 'Section 31 lockdown' → restrict to monitoring only

# 10) Monitoring & Metrics

# HQ Dashboards

* Node health, tunnel status, CPU/Mem/Disk, scan throughput
* Video ingest FPS, backlog, retention days, disk pressure on `/ha`
* Jarvis command success rate, error ratios, latency

# 11) CI/CD & Versioning

# Process

* Monorepo (`ogre‑armageddon`) with `backend/`, `frontend/`, `agent/`, `infra/`, `docs/`
* Semantic versioning; changelog per release; signed tags
* Image builds for Agent are immutable; staged rollout to canary node first
* Backups tested monthly; restore drills

# 12) Nice Additions (Highly Recommended)

# Quality of Life

* Node enrollment QR codes (printable) that embed pubkey and labels
* In‑UI JSON export/import for policy bundles and mode presets
* One‑click 'Section 31 Mission' wizard that preloads stealth configs
* Hardware watchdog on Agent for auto‑reboot if unresponsive
* Optional Tailscale support alongside native WireGuard

# 13) To‑Do Signoff Checklist

* ☐ HQ ready: Docker, UI, Jarvis, WG server, logging
* ☐ Disks mounted: `/`, `/ai`, `/srv`, `/ha` (future)
* ☐ Agent image: boots, tunnels, shows heartbeat
* ☐ Modes verified: Regular, Section 31, Borg, Scorched Earth
* ☐ Safeties tested: kill‑switch, lockout detect, rollback
* ☐ Backups & restore drill completed