SCHÉMA DE PROTECTION MAXIMALE

Architecture de Sécurité Souveraine & Sûreté Globale

Programme Gouvernemental LAZIM FALOOS — Supervisé par le Dr. Moumen Ouarghin

1. Protection Spatiale et Globale (Niveau Supérieur)

- **Protection Intégrale Ancrée :** Déploiement d'un bouclier cybernétique centralisé assurant la surveillance en temps réel et la défense périmétrique de l'écosystème global.
- **Diodes Laser de Sécurité :** Établissement d'une liaison optique descendante et ascendante hautement sécurisée par constellation de satellites en orbite basse (**Liaison LEO**), garantissant l'immunité face aux interceptions terrestres classiques.

2. Architecture de Sécurité Multi-Couches

L'infrastructure technique est structurée en trois couches défensives étanches, conçues pour neutraliser les menaces de manière séquentielle :

A. Couche Périphérique (17CYBER)

Cette première ligne de défense gère le filtrage et la surveillance des flux aux frontières du réseau.

- **Masquage Split-Horizon :** Cloisonnement strict des requêtes et tables de routage DNS internes et externes pour interdire toute tentative de cartographie ou de reconnaissance des infrastructures.
- **Diagnostic IC :** Évaluation continue et automatisée de l'intégrité des composants système et détection proactive des anomalies de comportement.

B. Couche Furtive (DNS Privé)

Zone d'ombre technique visant à opacifier les données applicatives et l'infrastructure de routage.

- **Anonymisation sous Actifs :** Chiffrement dynamique et dissimulation complète des identifiants d'actifs, rendant invisibles les transactions et les communications internes.
- **Coordination Institutionnelle :** Passerelle d'alerte et de liaison directe avec les forces de l'ordre (Police & Gendarmerie) pour la réponse aux incidents critiques.

C. Couche Physique (Diode Matérielle)

Le noyau de sécurité ultime assurant la protection absolue des données les plus sensibles.

- **Rupture d'Isolement sous Actifs :** Séparation physique et galvanique totale entre les réseaux de confiance et les réseaux externes non sécurisés.
- **Exfiltration Impossible :** Flux de données unidirectionnel strict appliqué par matériel (hardware-enforced), interdisant physiquement tout retour ou fuite de flux d'informations vers l'extérieur.

3. Matrice de Vérification de l'État Défensif

Type de Menace / Analyse	État de Sécurité	Définition Opérationnelle et Niveau de Résistance
Scan & Exploitation DNS	IMPERMÉABLE	Les serveurs DNS racine sont masqués. Aucune cartographie externe n'est techniquement réalisable.
Interception Terrestre	IMMUNE	Les infrastructures de transit au sol utilisent un chiffrement de bout en bout de classe militaire.
Exterception Terrestre	NICHE PHYSIQUE	Le confinement des signaux et des risques est circonscrit au sein d'un périmètre matériel contrôlé.
Exfiltration de Données	BLOQUÉ PHYSIQUE	Sécurité absolue garantie par diode matérielle. Le matériel empêche physiquement l'inversion du flux.
Attaque Informatique Quantique	SCELLÉ	Intégration d'algorithmes de cryptographie post-quantique (Kyber / Dilithium) résistant aux calculateurs de future génération.

ANNEXE D — SÉCURITÉ POST-QUANTIQUE

```
Kyber — Dilithium — Enclaves — Chiffrement
```

ANNEXE E — MATRICE DE VÉRIFICATION

```
DNS — Interception — Exfiltration — Quantique
```