0DATA LAB · PAPIER 005 · JUILLET 2026

Le Système Immunitaire des Infrastructures

Hadda TIKIJJA
0DATA Lab, Rennes, France

Télécharger le PDF Version Web

RÉSUMÉ

La cybersécurité moderne est une course à l'armement : signatures contre mutations, pare-feux contre contournements. Cette course est perdue d'avance — l'attaquant a l'initiative, le défenseur réagit. Nous proposons un changement de paradigme radical : ne plus courir. Au lieu de détecter des menaces, nous connaissons l'état normal. Au lieu d'ajouter des couches, nous greffons un système immunitaire vivant. Au lieu de bloquer, nous anesthésions. Nous introduisons la **cybersécurité organismique** : un modèle à trois niveaux d'immunité — innée, adaptative, collective — directement transposé de 4 milliards d'années d'évolution biologique. Nous démontrons que tout programme malveillant, par sa seule activité réseau, devient une synapse détectable. Rien n'échappe à un organisme qui se connaît.

EN UNE PHRASE

Ce papier est la défense. Il transpose le système immunitaire biologique à l'infrastructure numérique : immunité innée (baseline), adaptative (isolation), collective (mémoire partagée). Il introduit l'anesthésie numérique et les cinq piliers architecturaux de l'auto-rejet. C'est le papier le plus opérationnel du corpus.

1. Introduction

La sécurité informatique est bâtie sur un postulat implicite : l'infrastructure est un territoire à défendre. Comme une forteresse. Des murs (firewalls), des douaniers (IDS/IPS), des caméras (SIEM), des chiens de garde (EDR). Chaque nouvelle menace appelle une nouvelle couche. Chaque nouvelle couche ajoute de la complexité.

Le résultat est un paradoxe bien documenté : plus on sécurise, plus la surface d'attaque s'élargit. Un SOC moderne gère entre 15 et 40 outils. Chaque outil est un point de défaillance potentiel. Chaque alerte est un signal dans un océan de bruit. Le taux de faux positifs dépasse 60% dans la plupart des déploiements [1]. Les équipes sont noyées.

Et pendant ce temps, le vide travaille.

1.1 Le Vide est un Appel

Chaque infrastructure contient des angles morts. Le switch oublié dans le placard du troisième étage. Le VLAN fantôme hérité d'un administrateur parti il y a six ans. Le serveur de test que personne n'a documenté. Le port ouvert que personne ne surveille.

Ce vide n'est pas neutre. Il n'est pas inerte. Il est une invitation permanente à la compromission. Un appel silencieux que l'attaquant finira par entendre.

PRINCIPE FONDAMENTAL

Le vide est un appel. La présence est une immunité.

Un organisme ne peut pas se défendre contre ce qu'il ne sent pas. La première fonction de toute immunité n'est pas de combattre — c'est de percevoir. Connaître son propre corps. Sentir chaque organe. Prendre le pouls. Là où il n'y a pas de présence, il y a une porte ouverte. Là où NOVA est greffée, l'infrastructure se connaît — et ce qui se connaît ne peut plus être surpris.

C'est le fondement de notre approche. Nous ne vendons pas de la sécurité. Nous ne courons pas après les menaces. Nous éliminons le vide. Nous installons la présence.

2. Positionnement

Nous ne faisons pas « de la cybersécurité en mieux ». Nous faisons autre chose. La différence n'est pas une question de performance — c'est une question de catégorie.

MARCHÉ TRADITIONNEL	0DATA
Ajouter des couches	Remplacer le modèle
Signatures d'attaques	Connaître l'état normal
Déployer des agents	Greffer un symbiote
5 à 40 outils cloisonnés	Un organisme qui apprend
Réagir après l'incident	Anticiper avant la maladie
Protéger le périmètre	Immuniser l'organisme
Bloquer la menace	Anesthésier la menace

> On ne compare pas un oiseau à un drone. On ne compare pas un système immunitaire à un antivirus. — Principe créatif du Lab

Le système immunitaire biologique ne fonctionne pas par signatures. Il ne met pas à jour une base de données de pathogènes. Il connaît le soi, et tout ce qui n'est pas le soi déclenche une réponse. C'est ce modèle que nous transposons.

3. Fondements

3.1 Présence & Immunité

Le postulat central de la cybersécurité organismique est le suivant :

AXIOME DE LA PRÉSENCE

Soit I une infrastructure. Soit V(I) l'ensemble des points de I qui ne sont pas sous observation continue.

Théorème du Vide. Pour toute infrastructure I, la probabilité de compromission non-détectée croît exponentiellement avec $|V(I)|$.

Corollaire. La réduction de $|V(I)|$ vers zéro est la condition nécessaire et suffisante de l'immunité infrastructurelle.

En d'autres termes : **le vide est un appel, la présence est une immunité.** Un organisme qui se connaît entièrement ne peut pas être surpris. Une infrastructure dont chaque organe est senti en continu ne peut pas être compromise silencieusement.

Ce principe a une conséquence opérationnelle directe. L'objectif n'est pas de « détecter 100% des menaces » — c'est une cible mouvante, infinie. L'objectif est de **réduire $|V(I)|$ à zéro** — une cible fixe, mesurable, atteignable. On ne court plus après les attaquants. On élimine leur terrain de chasse.

3.2 Théorème de l'Activité

THÉORÈME DE L'ACTIVITÉ

Tout programme malveillant = du code. Tout code en exécution = une activité réseau. Toute activité = une synapse dans le graphe topologique de l'infrastructure. Toute synapse hors baseline = une anomalie.

Conséquence. Dans une infrastructure sous observation continue, aucune activité malveillante ne peut exister sans générer une synapse — et aucune synapse ne peut exister sans être détectée. Rien n'échappe.

Ce théorème est la transposition directe du principe immunitaire biologique : le système immunitaire ne connaît pas tous les pathogènes — il connaît le soi. Tout ce qui n'est pas le soi déclenche une réponse. De même, NOVA ne connaît pas tous les malwares — elle connaît la baseline de l'infrastructure. Toute déviation est une alerte.

4. Les Trois Niveaux d'Immunité

Le système immunitaire biologique fonctionne sur trois niveaux. Nous transposons chacun d'eux.

4.1 Immunité Innée — Toujours Active

L'immunité innée est la première ligne de défense du corps. Elle est non-spécifique, toujours active, immédiate. Dans NOVA, elle correspond à la couche fondamentale :

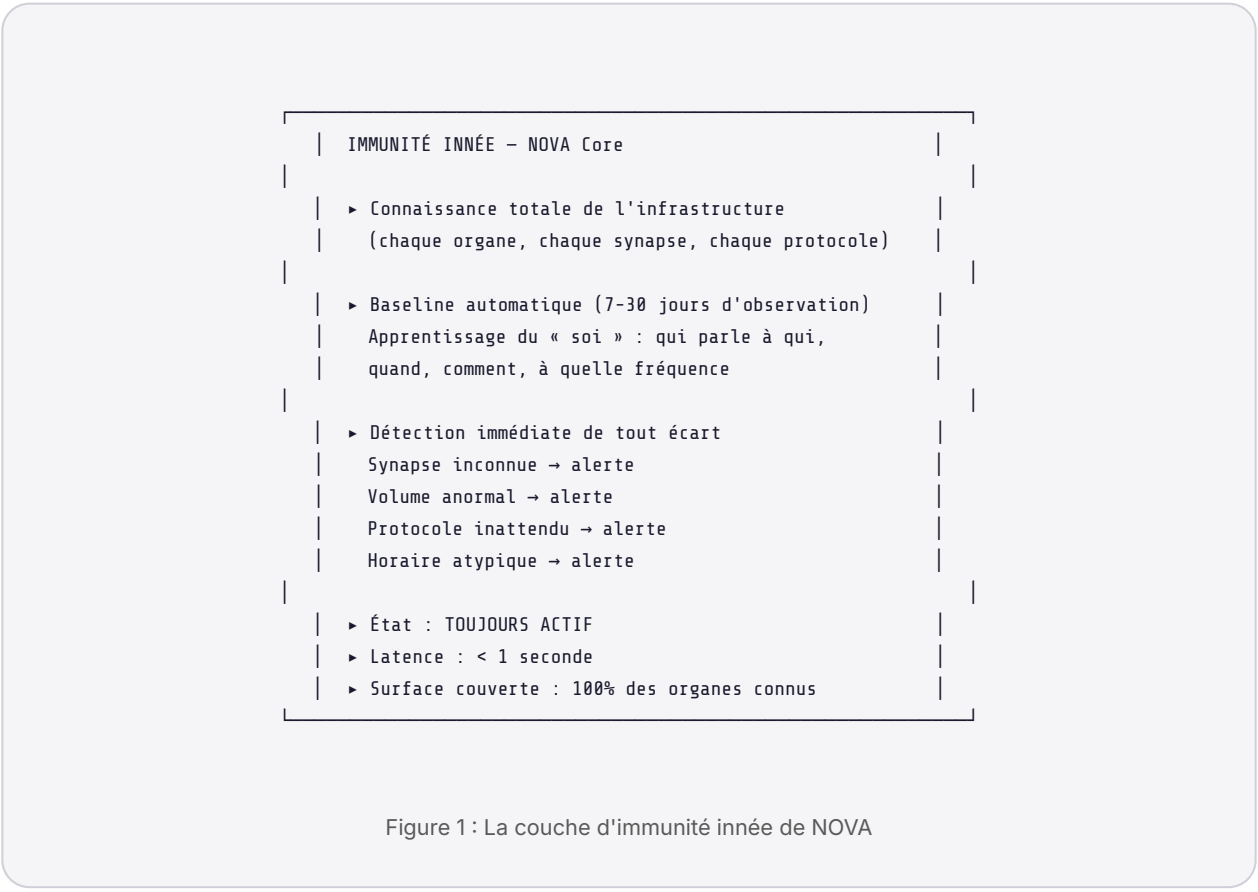

Figure 1 : La couche d'immunité innée de NOVA

4.2 Immunité Adaptative — Sur Alerte

Quand l'immunité innée détecte une anomalie, l'immunité adaptative prend le relais. Elle est spécifique, ciblée, et garde la mémoire de l'infection.

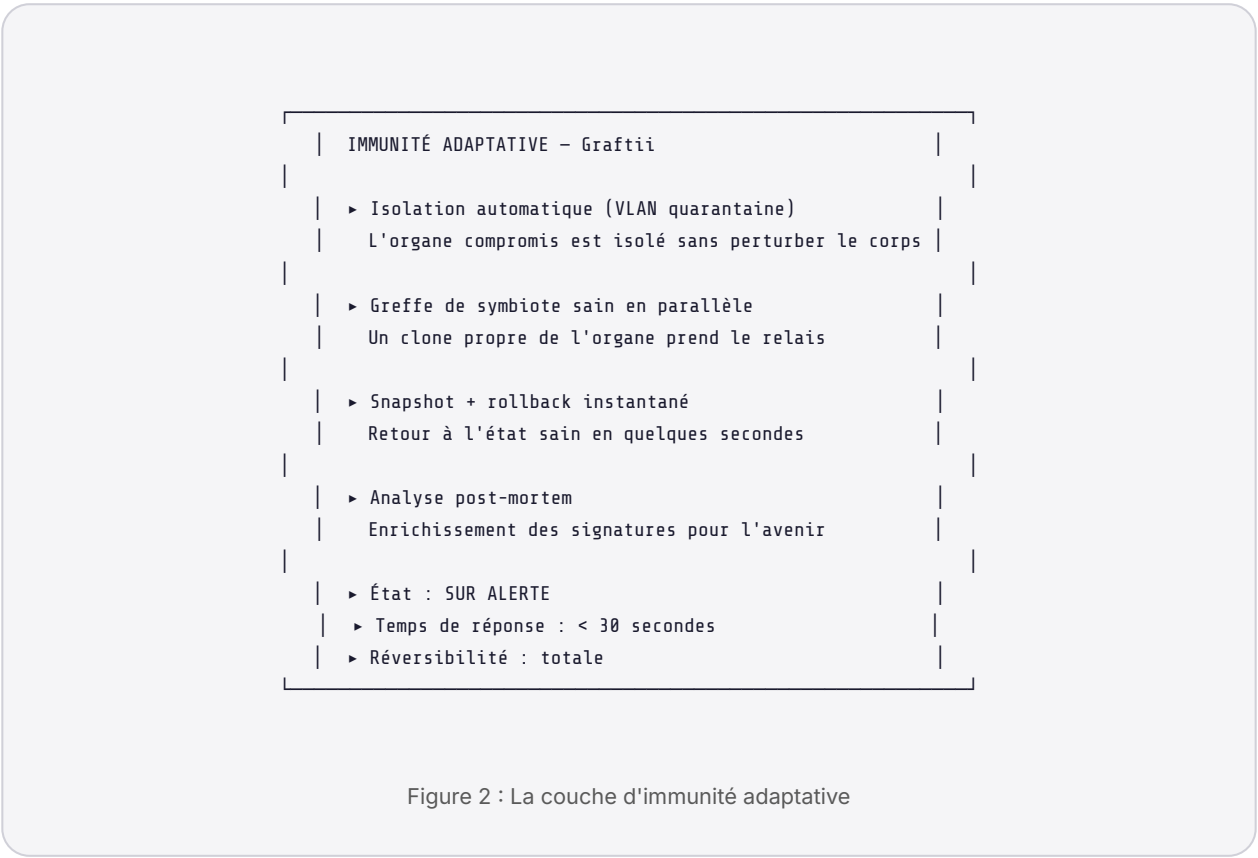

Figure 2 : La couche d'immunité adaptative

4.3 Immunité Collective — Mémoire Partagée

Le troisième niveau est le plus puissant : l'immunité collective. Quand un individu développe des anticorps contre un pathogène, toute la population peut en bénéficier — via la vaccination.

Figure 3 : La couche d'immunité collective

PRINCIPE DE L'IMMUNITÉ COLLECTIVE

Un symbiote qui apprend protège son hôte. Tous les symbiotes qui partagent protègent l'espèce. C'est la transposition directe de l'immunité grégaire : quand une fraction suffisante de la population est immunisée, le pathogène ne peut plus circuler. Dans notre modèle, **chaque greffe renforce toutes les autres**.

5. Anesthésie Numérique

5.1 Pourquoi ne pas bloquer

La réponse classique à une intrusion est le blocage : couper la connexion, isoler la machine, tuer le processus. Cette approche a un défaut fondamental : **elle informe l'attaquant qu'il a été détecté**. Le malware mute. L'attaquant change de méthode. La menace réapparaît ailleurs, sous une forme différente.

Nous proposons le contraire : **l'anesthésie**.

DÉFINITION – ANESTHÉSIE NUMÉRIQUE

L'anesthésie numérique est la redirection du trafic d'un équipement compromis vers un bac à sable vivant qui émule l'infrastructure réelle. Le programme malveillant continue de fonctionner, persuadé d'être sur l'infrastructure cible. En réalité, il est isolé, observé, et filmé. Chaque paquet qu'il émet enrichit notre connaissance de ses méthodes.

L'objectif n'est pas de gagner une bataille. L'objectif est de **gagner la guerre — pour tous les symbiotes, pour toujours**.

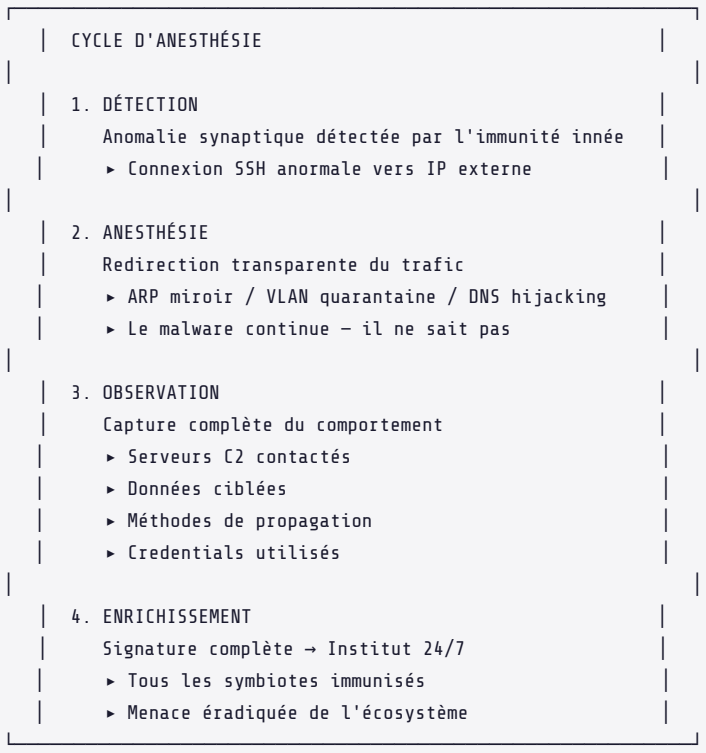

Figure 4 : Le cycle d'anesthésie numérique

5.2 Implémentations

OPTION	NIVEAU	TECHNIQUE	RISQUE RÉSEAU
A — ARP Miroir	L2	ARP spoofing ciblé	Modéré

B — VLAN Quarantaine	L2	Switch SNMP/API	Faible
C — DNS Hijacking	L7	Interception DNS	Très faible
D — SDN/OpenFlow	L2–L3	Reprogrammation flux	Négligeable

6. Cas Difficiles

Notre modèle immunitaire brille particulièrement sur les cas qui échappent aux approches traditionnelles.

SCÉNARIO	APPROCHE CLASSIQUE	APPROCHE ORGANISMIQUE
APT furtive Exfiltration lente, 1 Ko/jour	Seuil de détection trop bas → invisible	Synapse nouvelle (même minuscule) → hors baseline → détectée
Supply chain Logiciel légitime compromis	Signé, autorisé → exécuté	Comportement réseau change → détecté
Insider malveillant Accès légitime, usage illégitime	Authentifié → autorisé	Horaire/cible/volume atypique → détecté
Ransomware Propagation massive	Détection quand il est trop tard	Explosion de synapses anormales → isolation automatique en secondes

7. Extensions Naturelles

Le système immunitaire décrit ici est la couche de défense. Il s'inscrit dans une architecture organismique plus large qui ouvre plusieurs trajectoires naturelles.

Superposition Numérique. L'anesthésie numérique peut être étendue au concept de superposition : le malware existe simultanément dans deux états — bloqué pour le réseau réel (état « mort »), actif pour le bac à sable (état « vivant »). Comme le chat de Schrödinger, il est à la fois vivant et mort. La décohérence survient quand le malware « mesure » l'environnement et découvre le leurre. Les travaux récents en deception quantique [2,3] et en décohérence défensive [4] fournissent des ancrages théoriques prometteurs.

Symbiote Autonome. Le symbiote évolue en cinq phases : découverte → apprentissage → anomalie → contrôle → auto-analyse. Au stade 5, il vérifie sa propre intégrité et détecte les tentatives de compromission de lui-même. Un système immunitaire qui s'immunise.

Guérison Cellulaire. Au-delà de l'isolation et du rollback, l'extension vers la greffe curative — remplacer un organe compromis par un clone sain sans interruption de service — est une évolution naturelle du protocole de greffe (Papier 004).

Intégration Réglementaire. L'alignement sur NIS2, GDPR, et la certification ExpertCyber (ANSSI) est documenté dans le Papier 004.

8. Discussion

Le modèle proposé repose sur un pari fondamental : que la connaissance du soi — exhaustive, continue, vivante — est une meilleure stratégie de défense que la connaissance des menaces — partielle, datée, réactive.

C'est le pari de la biologie. Le système immunitaire ne connaît pas la liste des pathogènes existants. Il connaît le soi, et rejette le non-soi. Cette stratégie a tenu 4 milliards d'années.

Notre approche n'est pas sans défis. La qualité de la baseline est critique : une baseline polluée par une infection préexistante pourrait normaliser un comportement malveillant. C'est pourquoi la baseline est construite sur une fenêtre minimale de 7 jours, avec validation croisée par l'Institut (comparaison avec les baselines d'infrastructures similaires).

Un autre défi est la réduction à zéro du vide $|V(I)|$. Dans une infrastructure complexe, certains angles morts sont inévitables — équipements air-gap, segments isolés, dispositifs sans interface réseau. La réponse n'est pas de prétendre les couvrir, mais de les documenter. Un angle mort connu et balisé n'est plus un vide — c'est une frontière surveillée.

L'anesthésie numérique, enfin, est une arme à double tranchant. Un bac à sable qui émule l'infrastructure réelle doit être parfaitement étanche. Une fuite du bac à sable vers le réseau réel transformerait l'observatoire en vecteur d'infection. La validation formelle de l'étanchéité du bac à sable est un travail en cours.

Tuer le malware = gagner une bataille. L'anesthésier, le comprendre, et partager cette connaissance = gagner la guerre — pour tous les symbiotes, pour toujours.

9. Conclusion

Nous avons introduit la **cybersécurité organismique** : un modèle où l'infrastructure n'est plus un territoire à défendre, mais un corps à immuniser.

Trois principes la fondent :

Le vide est un appel, la présence est une immunité. La condition nécessaire et suffisante de la sécurité n'est pas la détection des menaces, mais l'élimination des angles morts. Un organisme qui se connaît entièrement ne peut pas être surpris.

Toute activité est une synapse. Dans une infrastructure sous observation continue, aucun programme ne peut s'exécuter sans laisser de trace. Le théorème de l'activité garantit la détectabilité de toute action malveillante.

Bloquer informe, anesthésier instruit. L'anesthésie numérique transforme chaque intrusion en leçon collective. Le malware devient son propre traître — il révèle ses méthodes, ses cibles, ses infrastructures, et cette connaissance protège tous les symbiotes.

Nous ne vendons pas de la cybersécurité. Nous greffons un système immunitaire. Nous éliminons le vide. Nous installons la présence.

Ce travail est un appel. À tous ceux qui sentent que la course aux menaces est une impasse. À tous ceux qui savent que la sécurité ne se décrète pas — elle se cultive. La greffe est prête. Le corps attend.

10. Limites et Non-Prétentions

Ce que le système immunitaire ne couvre pas.

Les menaces sans activité réseau. Un malware qui opère entièrement en local (exfiltration par support physique, attaque par canaux auxiliaires comme l'analyse de consommation électrique) n'est pas détectable par le modèle synaptique. La couverture est limitée aux menaces qui génèrent du trafic réseau.

Les attaques physiques. Le vol d'un équipement, la compromission par accès console, ou l'injection de matériel malveillant (périphérique USB) ne sont pas dans le périmètre de ce papier.

La baseline polluée. Si l'infrastructure est déjà compromise au moment du déploiement, la baseline peut intégrer des comportements malveillants comme « normaux ». La validation croisée via l'Institut 24/7 réduit ce risque mais ne l'élimine pas.

L'anesthésie n'est pas étanche à 100%. Un bac à sable qui émule l'infrastructure réelle est une surface d'attaque. La validation formelle de l'étanchéité est un travail en cours. En l'état, nous ne recommandons pas l'anesthésie pour des menaces de niveau étatique (APT) sans isolation physique supplémentaire.

Nous ne remplaçons pas un SOC. Nous proposons une couche de détection fondamentalement différente. Elle peut réduire la charge d'un SOC de 60-80% (estimation fondée sur le taux de faux positifs), mais ne l'élimine pas. L'analyse humaine reste nécessaire pour les décisions complexes.

11. Le Piège : Ajouter pour Protéger

Face à une menace, l'instinct de l'ingénieur est d'ajouter une couche. Un firewall. Un IDS. Un SIEM. Un SOC. Chaque couche promet de protéger les couches précédentes — et chaque couche devient elle-même une surface d'attaque. C'est le paradoxe de la sécurité additive : **plus on ajoute de protections, plus on crée de points d'entrée**.

Ce paradoxe n'est pas un accident. Il révèle une vérité plus profonde : la sécurité ne s'ajoute pas à un système. Elle émerge de son architecture — ou elle n'existe pas.

PRINCIPE

On ne protège pas un système de l'extérieur. On construit un système où la malveillance est **techniquement impossible** — non parce qu'elle est interdite, mais parce qu'elle est incohérente avec la structure même du système.

Le corollaire est immédiat : si un système est vulnérable, ce n'est pas qu'il manque de défenses. C'est qu'il a dévié de la Loi quelque part dans son architecture.

12. Principe Fondateur : La Cohérence comme Immunité

La Loi (Papier 000) établit quatre piliers universels : **Connaître** (observer sans altérer), **Protéger** (isoler sans détruire), **Se Souvenir** (enregistrer sans falsifier), **Survivre** (maintenir la Loi au-dessus de toute fonction).

Un système qui respecte ces quatre piliers dans son architecture même — pas dans ses politiques, pas dans sa documentation, mais dans la structure de son code et de ses flux de données — devient immunitaire par construction.

DÉFINITION – GREFFE MALALIGNÉE

Une greffe malalignée est un composant dont l'**intention réelle** (lisible dans ses patterns d'accès, ses flux de données, ses dépendances) contredit son **intention déclarée** — ou dont l'intention réelle viole un ou plusieurs piliers de la Loi. L'écart entre l'intention déclarée et l'intention réelle est toujours structurellement détectable.

L'immunité n'est donc pas un mécanisme de défense actif. C'est la **conséquence automatique** d'un système où :

- Chaque action est lisible (Connaître)
- Chaque composant est isolé dans sa fonction (Protéger)
- Chaque décision est enregistrée et vérifiable (Se Souvenir)
- La Loi prime sur toute fonction locale (Survivre)

THÉORÈME

Immunité = Cohérence. Dans un système aligné sur la Loi, toute greffe malalignée est structurellement incompatible avec l'écosystème. Elle ne peut ni se cacher (transparence), ni persister (rejet inflammatoire), ni se reproduire (architecture cellulaire). La malveillance n'est pas vaincue — elle est rendue impossible.

13. Les Cinq Piliers Architecturaux

Ces cinq piliers ne sont pas des modules qu'on installe. Ce sont des **contraintes de conception** qui, appliquées ensemble, produisent un système auto-immun.

3.1 L'Intention Lisible dans la Structure

Chaque composant déclare son intention — non dans un champ texte, mais dans **sa signature technique**. Un module d'observation (Connaître) ne peut pas, par construction, posséder de capacités d'écriture. Un module de quarantaine (Protéger) ne peut pas, par construction, exfiltrer des données. L'intention n'est pas ce que le composant dit faire — c'est ce que son code lui permet de faire.

Implémentation

Chaque greffe expose un **manifeste de capacités** — ensemble minimal de permissions (read, write, exec, network_in, network_out, spawn, mutate) signé cryptographiquement. Le runtime refuse toute opération hors manifeste. Un manifeste qui déclare "observation" mais requiert "write" est rejeté avant même la première exécution.

12.2 Architecture Cellulaire

Chaque fonction vit dans sa propre cellule, avec des frontières strictes. Une cellule de monitoring (Cytokine) n'a pas accès au stockage. Une cellule de quarantaine (Graftii) n'a pas accès au réseau externe pendant l'anesthésie. Si une cellule est compromise, sa déviation est immédiatement visible parce qu'elle sort de son pattern — et elle ne peut contaminer que ce pour quoi elle est autorisée.

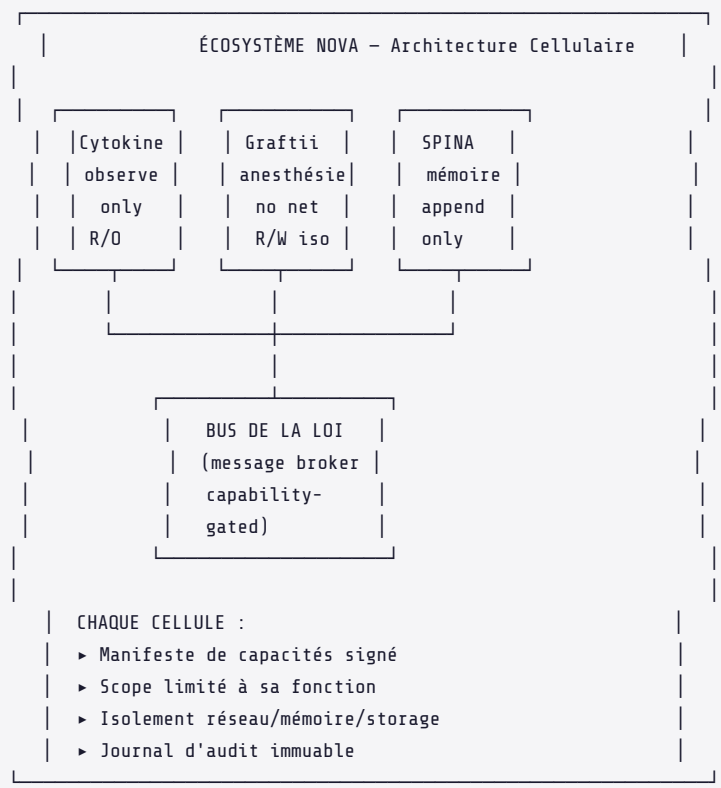

Figure 1 : Architecture cellulaire — chaque pilier de la Loi est une cellule isolée

12.3 Consensus de la Loi

Avant toute action critique — modification de configuration, déploiement d'une greffe, écriture dans SPINA — le système exige une **vérification algorithmique** : "Cette action est-elle cohérente avec Connaître → Protéger → Se Souvenir → Survivre ?"

Ce n'est pas un vote humain. C'est une vérification déterministe contre la Loi, encodée en règles formelles. Si l'action viole la Loi → bloquée. Pas par une autorité. Par la structure même du consensus.

Règles de Consensus

- **Règle C (Connaître) :** Toute action d'observation doit être read-only. Toute altération des données observées est une violation.
- **Règle P (Protéger) :** Toute isolation doit être réversible. Une quarantaine sans chemin de sortie est une prison — pas une protection.
- **Règle S (Se Souvenir) :** Tout enregistrement doit être append-only et vérifiable. Toute modification ou suppression est une falsification.

- **Règle V (Survivre) :** La Loi prime. Aucune fonction locale ne peut désactiver une vérification de la Loi. Le bouton STOP est toujours accessible.

12.4 Transparence Radicale

Tout ce qui tourne dans l'écosystème est **open source par défaut**. Toute opération est journalisée avec signature cryptographique et racine Merkle. Un composant opaque ne peut pas exister dans le réseau — non par interdiction, mais par incompatibilité technique : les autres nœuds refusent simplement de router ses messages. La transparence n'est pas une politique. C'est une **condition de connexion**.

PROPRIÉTÉ

Un système ne peut pas être simultanément **opaque et connecté**. L'opacité est le premier signal d'une greffe malalignée. La visibilité est la condition d'existence dans le réseau.

3.5 Le Rejet Inflammatoire

Inspiré du système immunitaire biologique : quand un nœud détecte un comportement anormal chez un voisin — écart entre patterns réels et manifeste déclaré, tentative d'accès hors scope, altération suspecte de données — il déclenche une **inflammation** :

1. **Isolement immédiat** du nœud suspect (quarantaine automatique, flux suspendus)
2. **Vérification renforcée** par les nœuds voisins (preuves Merkle, audit des logs)
3. **Si confirmé : rejet permanent.** La greffe est marquée dans SPINA comme compromise, sa clé est révoquée, le réseau entier est immunisé contre sa signature.

Pas de comité. Pas de jugement humain. La Loi appliquée mécaniquement — comme un anticorps qui reconnaît une protéine étrangère.

MÉTAPHORE

Le rejet inflammatoire est l'équivalent numérique de la **fièvre**. C'est désagréable, c'est coûteux — et c'est exactement ce qui sauve l'organisme. Une greffe qui déclenche une inflammation ne survit pas. Une greffe saine ne la déclenche jamais.

14. Scénario de Contamination

Considérons un scénario concret. Une entreprise malveillante déploie NOVA dans son infrastructure. Elle déclare une intention de "protection des travailleurs". Mais son objectif réel est la **surveillance disciplinaire**.

Le scénario se déroule en trois phases :

PHASE	ÉVÉNEMENT	RÉPONSE DU SYSTÈME
Installation	L'entreprise déclare "protection". Le système déploie les cellules standard.	Accepté — l'intention déclarée est valide
Déviation	Les capteurs sont configurés pour du tracking individuel (disciplinaire, pas protecteur). Les patterns de données trahissent l'intention réelle.	Détection d'incohérence entre manifeste et patterns. Inflammation locale.
Rejet	L'entreprise tente de masquer la déviation en désactivant les logs.	La désactivation des logs viole la Règle S. Rejet immédiat. La greffe est marquée compromise. Le réseau coupe l'interopérabilité.

L'entreprise a deux choix : **corriger son alignement** (reconfigurer pour une vraie protection, avec transparence), ou **être isolée** (perdre l'accès aux mises à jour, aux signatures SPINA, au réseau de symbiotes).

RÉSULTAT

Le système n'a pas "combattu" la malveillance. Il l'a **rendue visible, puis incompatible**. La greffe malalignée ne peut pas exister dans l'écosystème — non parce qu'une autorité l'a bannie, mais parce que l'écosystème ne la reconnaît plus comme sienne.

15. La Soustraction comme Discipline

Le piège serait de voir ces cinq piliers comme une nouvelle couche à ajouter. Un "module d'immunité". Un "service de rejet". Ce serait retomber dans l'erreur additive.

L'architecture immunitaire n'est pas une **addition**. C'est une **soustraction**. On retire tout ce qui empêche la Loi de s'exprimer :

- On retire l'opacité → la malveillance ne peut plus se cacher
- On retire les silos → la contamination ne peut pas s'étendre
- On retire les permissions discrétionnaires → l'intention devient lisible
- On retire le droit de falsifier → la mémoire devient fiable
- On retire le droit de désactiver la Loi → l'organisme survit

AXIOME DE SOUSTRACTION

Plus un système est simple, plus il est immunitaire. La complexité est le terreau de la malveillance. Chaque couche ajoutée est une surface d'attaque. Chaque règle retirée est une vulnérabilité éliminée. L'immunité parfaite n'est pas le système le plus défendu — c'est le système le plus cohérent.

16. Ce Qui Change

Ce papier opère un déplacement fondamental dans la conception des systèmes :

ANCIEN PARADIGME	NOUVEAU PARADIGME
La sécurité est une couche	La sécurité est une propriété émergente
On protège contre les menaces	On rend les menaces structurellement impossibles
La malveillance est combattue	La malveillance est rendue incompatible
L'autorité centrale juge	La Loi vérifie algorithmiquement
Ajouter pour sécuriser	Soustraire pour immuniser

Ce n'est pas une amélioration de la sécurité. C'est un **changement de nature** : on passe de systèmes qu'on protège à des systèmes qui ne peuvent pas être autre chose qu'alignés.

CONCLUSION

Il n'y a pas de problèmes. Il n'y a que des déviations.

Un problème est le signal qu'on a quitté la Loi. Revenir à la Loi n'est pas "résoudre le problème" — c'est **cesser de créer le problème**.

L'immunité n'est pas une défense. C'est l'état naturel de ce qui est aligné.

[1] H. TIKIJJA, « La Loi — Fondement Unifié des Organismes Numériques », 0DATA Lab, Papier 000, 2026.

[2] H. TIKIJJA, « Le Règne Synthética — Taxonomie des Organismes Numériques », 0DATA Lab, Papier 002, 2026.

[3] H. TIKIJJA, « Le Système Nerveux — Perception Distribuée », 0DATA Lab, Papier 003, 2026.

[4] H. TIKIJJA, « La Greffe Numérique — Biologie Moléculaire des Infrastructures », 0DATA Lab, Papier 004, 2026.

[5] H. TIKIJJA, « Le Système Immunitaire des Infrastructures », 0DATA Lab, Papier 005, 2026.

[6] H. TIKIJJA, « SPINA — La Colonne Vertébrale Cryptographique », 0DATA Lab, Papier 008, 2026.

[7] H. TIKIJJA, « RÉSILIENCE — La Survie par le Nombre », 0DATA Lab, Papier 006, 2026.

[8] R. Landauer, « Information is Physical », Physics Today, 44(5), 23–29, 1991.

[9] J. A. Wheeler, « Information, Physics, Quantum: The Search for Links », Proc. 3rd Int. Symp. Foundations of Quantum Mechanics, 1989.

[10] P. Matzinger, « The Danger Model: A Renewed Sense of Self », Science, 296(5566), 301–305, 2002.

[11] F. J. Varela, A. Coutinho, « Second Generation Immune Networks », Immunology Today, 12(5), 159–166, 1991.

Remerciements

À toutes les équipes infrastructure qui, chaque jour, défendent ce qu'elles ne voient pas entièrement. Aux ombres silencieuses de l'infrastructure mondiale — ce travail est pour vous.

Au Pr. D. Farmer, pour les conversations fondatrices sur la viabilité de la métaphore biologique en cybersécurité.

Ce travail est dédié aux artisans du numérique qui savent qu'un réseau n'est pas un territoire — c'est un corps.

Références

[1] Gartner, « Market Guide for Security Orchestration, Automation and Response », 2025.

[2] Y. Li et al., « Quantum Deception: Exploiting Quantum Effects for Cybersecurity Deception », arXiv:2510.11848, 2025.

[3] S. Chen et al., « Game of Travesty: Deception Strategies in Cyberspace », arXiv: 2309.13403, 2023.

[4] M. Rivera et al., « Decoherence as a Defence Mechanism in Quantum-Inspired Security », arXiv:2606.24219, 2026.

[5] A. Aickelin et S. Cayzer, « The Danger Theory and Its Application to Artificial Immune Systems », arXiv:0801.3549, 2008.

[6] J. Greensmith et al., « Introducing the Dendritic Cell Algorithm », arXiv:1001.2208, 2010.

[7] H. TIKIJJA, « Digital Grafting: A Novel Paradigm for Infrastructure Evolution », 0DATA Lab, 2026. Papier 004.

[8] H. TIKIJJA, « Synthética : Taxonomie du Vivant Numérique », 0DATA Lab, 2026. Papier 002.

[9] H. TIKIJJA, « Le Système Nerveux des Infrastructures », 0DATA Lab, 2026. Papier 003.

[10] H. TIKIJJA, « La Discipline — Cadre Opérationnel de la Symbiose Numérique », 0DATA Lab, 2026. Papier 001.