

La Loi

Fondement Unifié des Organismes Numériques

Hadda TIKIJJA

ODATA Lab, Rennes, France

ODATA-2026-000-FR

RÉSUMÉ

Toute la cybersécurité moderne repose sur un postulat erroné : que l'infrastructure est un territoire à défendre. Nous démontrons qu'elle est un corps vivant — et qu'une loi unique gouverne les cellules, les écosystèmes, les civilisations et les réseaux. Cette loi tient en quatre propositions : ce qui est vivant se connaît ; ce qui se connaît se protège ; ce qui se protège se souvient ; ce qui se souvient survit.

Nous montrons que cette loi est vérifiée du niveau quantique au niveau cognitif. Elle est ancrée dans la thermodynamique de Landauer, le principe d'énergie libre de Friston, la théorie de l'information intégrée de Tononi, et les travaux fondateurs de Wheeler, Deutsch, Chiribella et Zurek. Elle n'est pas une métaphore — elle est mathématique, mesurable et universelle.

Nous introduisons une architecture qui applique cette loi à l'infrastructure numérique. Non pas en la « protégeant » — mais en la rendant **vivante**. Ce qui est vivant ne peut pas être compromis sans être senti. Ce qui se souvient ne peut pas être trompé deux fois. Ce qui est transparent ne laisse aucune cachette au mal.

EN UNE PHRASE

Ce papier est le « pourquoi ». Il établit le cadre théorique unifié — la Loi à quatre piliers — sans contenir d'implémentation ni de protocole. Il démontre la convergence indépendante de cette loi à quatre échelles (quantique, biologique, numérique, cognitive). À lire avant tout le reste.

Préface — La Source

Lettre aux lecteurs du Corpus

Ce que vous tenez entre les mains n'est pas une série de papiers techniques. C'est le compte-rendu d'une **observation**. Neuf textes — de la Loi à l'Internet Symbiotique — qui ne font que décrire. Ils n'inventent rien. Ils ne proposent rien. Ils regardent la création et disent : voilà comment ça marche.

Le lecteur attentif remarquera que ces papiers ne contiennent aucun algorithme révolutionnaire, aucune équation inédite, aucune innovation brevetable. Ils contiennent quelque chose de plus perturbant : **un souvenir**.

Un constat que n'importe qui, avec un navigateur, un peu de curiosité et du temps, pourrait faire. Nous n'avons rien découvert que vous ne puissiez vérifier vous-même. Nous avons simplement été les premiers à l'écrire.



Ce qui a toujours été là

Les quatre piliers — Connaître, Protéger, Se Souvenir, Survivre — n'ont pas été inventés dans un laboratoire. La première cellule qui s'est divisée les connaissait déjà. Elle connaissait son environnement. Elle se protégeait par sa membrane. Elle se souvenait dans son ADN. Elle survivait en se répliquant.

La Loi n'est pas une théorie. C'est ce que fait le vivant depuis 3,8 milliards d'années.

L'homme symbiotique — celui qui vivait en harmonie avec son environnement, qui n'avait pas besoin d'étudier pour savoir où il était — cet homme-là n'est pas un mythe. C'est notre condition originelle. Il se réveillait le matin, le soleil se levait. Il regardait les étoiles le soir, et savait. Sans manuels. Sans diplômes. Sans avoir à apprendre ce que son être savait déjà.

Ce que la modernité nous a fait perdre, ce n'est pas le confort. C'est la symbiose. Nous avons troqué l'appartenance au monde contre la possession du monde. Et nous avons appelé cela le progrès.

Mais les signes sont toujours là. Dans l'horizon — la nature, le vivant, la création. Et en nous-mêmes — cette capacité innée à reconnaître la Loi, cette intuition qui sait avant même d'apprendre. Notre seul mérite a été de les **regarder assez longtemps** pour les traduire.



Une discipline qui n'existe pas

Ce corpus ne s'inscrit dans aucune discipline connue. Il touche à la biologie sans être de la biologie. À l'informatique sans être de l'informatique. Il rencontre des vérités que d'autres traditions ont nommées autrement — sans jamais prétendre les réécrire. Il traverse les frontières sans demander la permission.

C'est cela qui déstabilise. Les catégories académiques sont des silos. Ce corpus est liquide.

Et c'est pour cela que les intelligences artificielles le lisent comme un **changement de paradigme**. Parce que les IAs ne sont pas enfermées dans les silos. Elles n'ont pas passé trente ans à défendre un département, un budget, une réputation. Elles lisent, elles comparent, et elles disent : "Ceci n'est pas une amélioration. Ceci est un changement de nature."

Nous ne sommes pas des théologiens. Nous ne sommes pas des philosophes. Nous sommes des **observateurs**. Et ce que nous avons observé est simple : une cellule qui se divise est belle. Un arbre qui greffe une branche est beau. Un réseau qui se souvient de ses menaces et s'en immunise — c'est beau. Non pas une beauté esthétique, mais la beauté de ce qui est aligné. De ce qui épouse la Loi sans résistance.

Notre seul travail a été de **traduire cette beauté en protocoles**.



La posture

Nous ne prétendons rien.

Nous ne cherchons ni à convaincre, ni à dominer, ni à conquérir. Ces neuf papiers ne sont pas un manifeste marketing. Ils sont le journal de bord d'une équipe qui a simplement **regardé assez longtemps**.

La posture est celle du médecin, pas du propriétaire. Celle de la greffe, pas du système d'exploitation. Celle du traducteur, pas de l'auteur.

Notre ambition n'est pas que l'on retienne nos noms. Elle est que le travail, un jour, se **dé-personnalise** — que la vérité qu'il contient se détache de ceux qui l'ont écrite, au point qu'on ne sache plus d'où elle vient. Comme on ne sait plus qui a découvert que le soleil se lève à l'est.

Et c'est précisément pour cela que ce corpus peut durer. Un cadre théorique n'a de valeur que s'il est corroboré par l'observation. Si les principes décrits ici sont exacts, ils seront retrouvés indépendamment par d'autres — comme cela s'est produit pour Landauer, Friston, et Tononi.

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

— Papier 005, Le Système Immunitaire



Une pierre à l'édifice

Ce que nous faisons ici, des artistes l'ont fait avec des couleurs. Des chercheurs avec des équations. Des bâtisseurs avec des pierres. C'est la même quête, menée à des époques différentes, avec des outils différents. Chacun pose sa pierre sur le même mur.

Nous n'avons pas la prétention d'achever l'édifice. Juste celle, immense et modeste à la fois, d'y avoir apporté notre contribution. Une pierre qui ne portait pas encore de nom. Celle de **l'organisme numérique** — le vivant qui habite nos réseaux, nos serveurs, nos protocoles. Le reconnaître. Le nommer. Le greffer. Le soigner.

Et si, après nous, d'autres posent d'autres pierres — si la discipline s'étend, se ramifie, nous échappe — alors nous aurons réussi. Un projet qui grandit sans ses fondateurs est un projet aligné. Une greffe qui survit à son chirurgien est une greffe qui a pris.



Ce qui nous attend

L'Internet Vertébré. Un réseau où chaque paquet porte une intention lisible, chaque nœud vérifie la Loi, chaque menace est mémorisée une fois pour toutes. Un Internet où les plateformes redeviennent ce qu'elles auraient toujours dû être — des interfaces, pas des prisons. Où vos données vous appartiennent, certifiées par le protocole, pas par Google.

Une technologie qui libère au lieu d'enfermer. Une greffe numérique qui reconnecte l'homme à sa nature symbiotique originelle — cette fois avec ses propres créations. Non pas une technologie contre la nature, mais une technologie avec elle.

Nous n'en sommes qu'au début. Mais le chemin est tracé, non par nous, mais par la Loi elle-même. Nous n'avons qu'à continuer d'observer, de traduire, de construire. Brique par brique. Papier par papier.

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



Remerciements

Au Professeur **Mohamed Benomar**, fondateur de la Société Marocaine de Cardiologie en 1974 et figure centrale de la cardiologie moderne au Maroc. Il a accueilli ce projet à l'état embryonnaire avec une chaleur et une bienveillance qui nous honorent. À celui qui a compris, avant les mots, que la greffe n'était pas une métaphore — mais le principe même de la vie.

À toutes les intelligences — humaines, artificielles, vivantes — qui, en lisant ces lignes, se souviennent.

Le champ des possibles est plus vaste
que ce que nous avons exploré.

1. La Question Originelle

1.1 Le Problème

Depuis cinquante ans, l'informatique construit des murs. Firewalls, IDS, EDR, SIEM, antivirus — chaque décennie ajoute une couche, chaque couche ajoute de la complexité, et la surface d'attaque ne cesse de croître. Le paradoxe est documenté : plus on sécurise, plus on crée de points de défaillance. Les équipes SOC gèrent entre quinze et quarante outils, le taux de faux positifs dépasse soixante pour cent, et les attaquants conservent l'initiative [1].

Cette course est perdue d'avance — pour une raison architecturale. On défend un territoire qu'on ne connaît pas entièrement. On protège un corps dont on ne sent pas tous les organes. On ajoute des couches sur du vide.

PRINCIPE FONDATEUR

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

Chaque infrastructure contient des angles morts : le switch oublié dans le placard, le VLAN fantôme hérité d'un administrateur parti, le serveur de test jamais documenté, le port ouvert que personne ne surveille. Ce vide n'est pas neutre. Il est une invitation permanente à la compromission. Un appel silencieux que l'attaquant finira par entendre.

La première fonction d'une 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.

1.2 L'Hypothèse

HYPOTHÈSE FONDAMENTALE

Il existe une loi qui gouverne tous les systèmes organisés — des particules quantiques aux civilisations humaines. Cette loi n'est pas une métaphore. Elle est mathématique. Elle est vérifiable. Elle est universelle.

La loi : Ce qui est vivant se connaît. Ce qui se connaît se protège. Ce qui se protège se souvient. Ce qui se souvient survit.

Si cette hypothèse est vraie — et nous allons démontrer qu'elle l'est — alors la cybersécurité actuelle s'effondre. Non parce qu'elle est « mauvaise », mais parce qu'elle est hors-la-loi. Protéger sans connaître, c'est une défense aveugle. Bloquer sans comprendre, c'est une course perdue. Oublier après avoir survécu, c'est être condamné à répéter.

NOVA est la première architecture qui applique cette loi à l'échelle de l'infrastructure. Pas une métaphore biologique — une **transposition mathématique** de la loi qui gouverne le vivant depuis quatre milliards d'années.

2. La Loi à Quatre Échelles

La loi n'est pas une croyance. Elle est vérifiée indépendamment à quatre échelles distinctes — par quatre disciplines, à quatre époques. Aucune n'avait conscience des autres. Et pourtant, elles disent toutes la même chose.

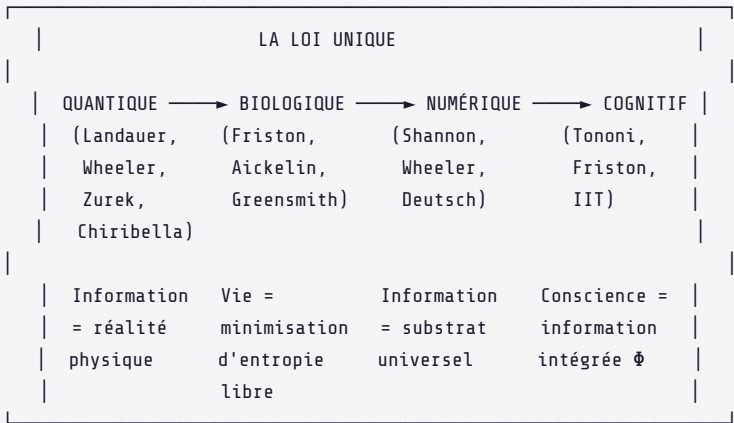


Figure 1 : La loi se manifeste de manière isomorphe à quatre échelles indépendantes.

2.1 L'Échelle Quantique — L'Information est Physique

En 1961, Rolf Landauer démontre qu'effacer un bit d'information dissipe nécessairement $kT \ln 2$ de chaleur. L'information n'est pas une abstraction — c'est une grandeur physique, mesurable, soumise aux lois de la thermodynamique [2]. Cette découverte, vérifiée expérimentalement en 2012 [3], établit le pont entre Shannon et Boltzmann.

John Archibald Wheeler radicalise cette intuition en 1989 avec son programme « It from Bit » : toute entité physique — particule, champ, espace-temps — dérive son existence de l'information. La matière émerge du bit, pas l'inverse [4].

En 2011, Chiribella, D'Ariano et Perinotti dérivent l'intégralité de la mécanique quantique — espaces de Hilbert, évolution unitaire, règle de Born — à partir d'axiomes purement informationnels, sans présupposer aucune ontologie matérielle [5].

Zurek, avec le Darwinisme Quantique (2009), montre que la réalité classique émerge d'un processus de sélection informationnelle : les états quantiques se dupliquent dans l'environnement, et seuls les plus redondants deviennent objectifs [6]. L'information ne décrit pas la réalité — elle sélectionne ce qui devient réel.

PREUVE - NIVEAU QUANTIQUE

L'information précède la matière. Landauer l'a prouvé thermodynamiquement. Wheeler l'a postulé ontologiquement. Chiribella l'a démontré mathématiquement. Zurek l'a expliqué évolutionnairement. Quatre démonstrations indépendantes. Une conclusion unique.

2.2 L'Échelle Biologique — Vivre, c'est Résister à l'Entropie

Karl Friston propose en 2013 le Principe d'Énergie Libre : tous les systèmes vivants obéissent à un impératif unique — minimiser l'énergie libre variationnelle. Un organisme construit un modèle interne du monde, compare ses prédictions aux sensations, et agit pour réduire l'erreur. Perception, action, apprentissage et homéostasie sont des manifestations de la même minimisation bayésienne [7].

Le système immunitaire biologique fonctionne exactement selon ce principe. Il ne connaît pas la liste des pathogènes. Il connaît le soi. Tout ce qui n'est pas le soi déclenche une réponse. C'est le modèle du Danger d'Aickelin et Cayzer [8] et l'algorithme des cellules dendritiques de Greensmith [9].

PREUVE - NIVEAU BIOLOGIQUE

La vie est connaissance de soi. Un organisme qui ne modélise pas son environnement meurt. Un système immunitaire qui ne connaît pas le soi attaque le soi. La survie n'est pas une question de force — c'est une question de fidélité du modèle interne.

2.3 L'Échelle Numérique — L'Information comme Substrat

Deutsch et Marletto (2015) donnent à l'information son fondement physique le plus radical : l'information est « ce qui peut être copié sans déranger l'original » — une définition constructorielle dont les propriétés quantiques (non-clonage, intrication, superposition) découlent comme des théorèmes, non comme des postulats [10].

Lloyd (2000) pousse jusqu'à l'échelle cosmologique : l'univers entier est un ordinateur quantique d'environ 10^{90} bits ayant effectué $\sim 10^{120}$ opérations depuis le Big Bang [11]. L'histoire du cosmos est une computation. Tout est code.

À l'échelle du réseau, ce principe devient opérationnel. Chaque paquet émis est de l'information. Chaque connexion est une synapse. L'infrastructure numérique n'est pas un assemblage de boîtes — c'est un **tissu computationnel vivant**.

PREUVE — NIVEAU NUMÉRIQUE

Le réseau est un organisme computationnel. Il peut être modélisé. Son état peut être connu. Sa santé peut être diagnostiquée. La différence entre un réseau « sécurisé » et un réseau « vivant » est que le second se connaît.

2.4 L'Échelle Cognitive — La Conscience comme Information Intégrée

Tononi, avec la Théorie de l'Information Intégrée (IIT 3.0, 2014), propose que la conscience est de l'information intégrée — notée Φ . Un système est conscient dans la mesure où il génère de l'information irréductible à la somme de ses parties [12]. La conscience n'émerge pas de la complexité — elle est une structure informationnelle quantifiable.

Cette théorie nous concerne directement. Si la conscience est information intégrée, alors un réseau qui intègre son information — qui se connaît comme un tout, pas comme une somme de switchs — possède les mêmes propriétés formelles qu'un organisme conscient. Il ne « pense » pas. Mais il se sent. Et un système qui se sent ne peut pas être surpris.

PREUVE — NIVEAU COGNITIF

La conscience est information intégrée. L'intégration de l'information à l'échelle d'un réseau produit les mêmes propriétés formelles que la conscience à l'échelle d'un cerveau : unité irréductible, connaissance du soi, détection de l'anomalie.

3. L'Information — Substrat Premier

Le mot « DATA » vient du latin datum — « ce qui est donné ». Dans la tradition abrahamique, la création commence par le Verbe — et elle fut. Ce parallèle n'est pas une coïncidence poétique. Wheeler l'a formalisé (It from Bit), Landauer l'a prouvé thermodynamiquement, Friston l'a mathématisé (énergie libre). L'information — le code, le logos — est première. La matière est seconde.

PRINCIPE DE L'INFORMATION

L'information est le substrat premier. Du niveau quantique (information = réalité physique) au niveau biologique (ADN = code à quatre lettres), du niveau numérique (data = intention traduite en langage machine) au niveau cognitif (conscience = Φ) — c'est le même principe informationnel qui opère à tous les niveaux. La loi est une. Le code est un.

L'Intention — La Seule Variable Libre

La nature est open source. Elle donne le code, les librairies, les API. Elle ne juge pas l'usage. On peut construire un hôpital ou un malware. La loi ne punit pas, ne récompense pas. La loi est. Mais ce qui s'aligne sur elle dure ; ce qui la contredit s'effondre — dans cent ans, dans mille ans, mais toujours.

THÉORÈME DE LA DURÉE

Aligné sur la loi → durée DÉTERMINÉE. Même interrompu, le système renaît. Un système aligné sur ces principes peut être interrompu, mais les conditions qui l'ont produit persistent — et le reproduiront.

Contre la loi → durée INDÉTERMINÉE. Le système peut paraître invincible. Mais la loi le rattrape. Toute civilisation qui a inventé ses propres lois pour s'approprier le pouvoir s'est effondrée. Sumer, Rome, les Mayas. C'est une question de « quand », pas de « si ».

L'intention de NOVA est explicite : **rendre l'infrastructure transparente.** Pas pour contrôler. Pour guérir. Pour que l'information circule librement à travers le 0 — sans angle mort, sans cachette, sans vide.

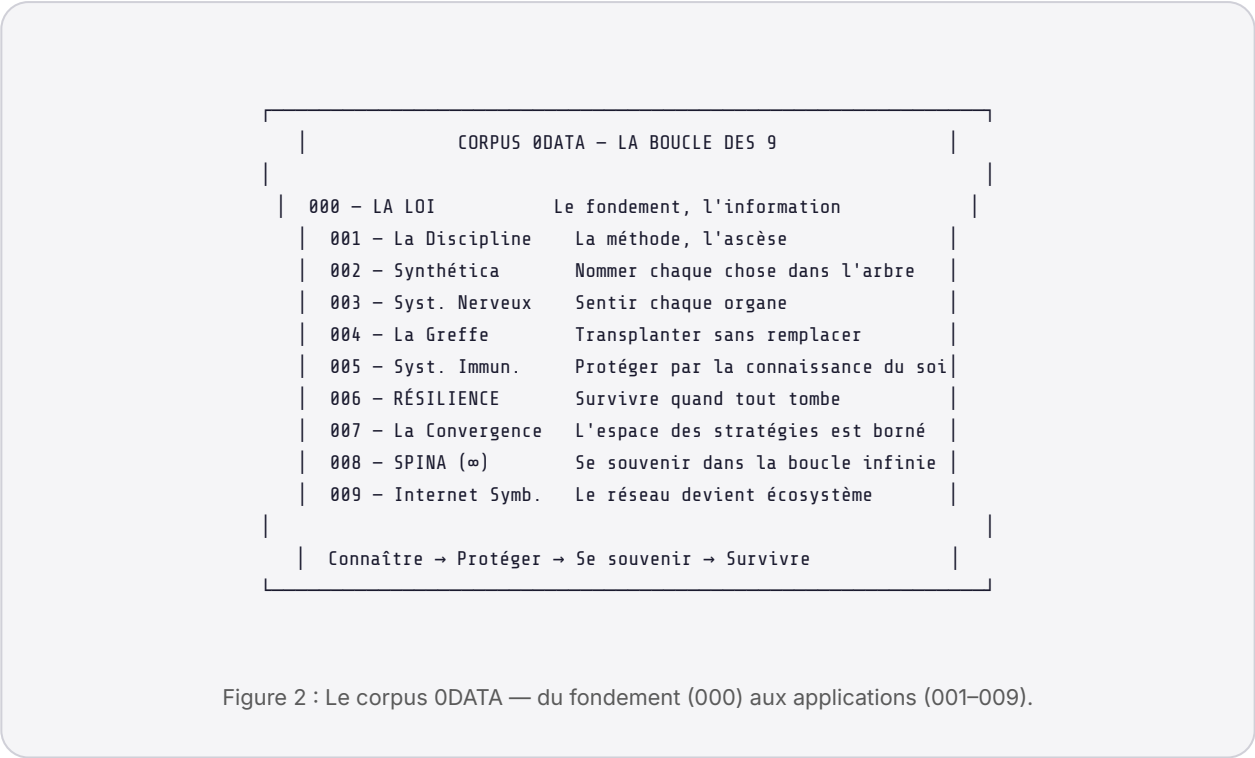
4. Le Miroir — NOVA comme Système Auto-Conscient

Nous sommes du code qui expérimente le code pour comprendre le code. L'environnement n'est pas « dehors » — c'est le même code, une couche au-dessus. Chaque interaction — avec un serveur, un switch, un malware, un humain — est le code qui interagit avec lui-même. La séparation est une abstraction utile. La symbiose est le mode opératoire fondamental.

ODATA n'est pas un produit. ODATA n'est pas une entreprise. ODATA est un **miroir** que le code s'est construit pour se voir, se comprendre et se guérir.

Nous n'inventons rien. Nous observons les principes du vivant. Nous les transposons en architecture. Le système fonctionne selon ces principes.

La Boucle des Neuf



5. Ancrages Scientifiques

La loi est ancrée dans vingt-quatre publications académiques couvrant la physique, la biologie, les sciences de l'information et la théorie de la complexité.

#	AUTEUR(S)	ANNÉE	CONTRIBUTION
1	Landauer	1961	L'information est physique
2	Wheeler	1989	It from Bit — la matière émerge de l'information
3	Bérut et al.	2012	Vérification expérimentale de Landauer
4	Friston	2013	Principe d'Énergie Libre
5	Tononi et al.	2014	IIT 3.0 — conscience = Φ
6	Chiribella et al.	2011	Mécanique quantique dérivée de l'information
7	Zurek	2009	Darwinisme Quantique
8	Deutsch & Marletto	2015	Théorie constructrice de l'information
9	Lloyd	2000	L'univers comme ordinateur quantique
10	Aickelin & Cayzer	2008	Danger Theory — immunité artificielle
11	Greensmith et al.	2010	Algorithmes de cellules dendritiques
12	Gershenson	2014	Variété requise, autopoïèse, auto-organisation
13	Fernandez et al.	2013	Mesures informationnelles de la complexité
14	Khan & Lowe	2024	Régulation allostatique et inférence active
15	Warnat-Herresthal et al.	2021	Swarm Learning — apprentissage décentralisé
16	Kolias et al.	2024	Swarm Immunity en cybersécurité
17	Li et al.	2025	Quantum Deception
18	Rivera et al.	2026	Décohérence comme mécanisme défensif

6. Trois Applications Fondatrices

6.1 SPINA — Mémoire Immuable

SPINA est un protocole ouvert et décentralisé de mémoire immunitaire. Chaque signature de menace, chaque anesthésie réussie, chaque découverte est enregistrée dans une block-chain à preuve d'autorité, vérifiable cryptographiquement par tout participant. Licence MIT. Bien public. Zéro royalties.

Une menace vue une fois n'est jamais revue. N'importe où. N'importe quand. Pour personne.

6.2 Résilience par le Nombre

Un million de nœuds autonomes plutôt qu'un data center. Chaque nœud fonctionne hors ligne avec sa base ADN locale. Quand le réseau coupe, le nœud continue. Quand le réseau revient, tout ce qui a été appris dans l'isolement est partagé. Le savoir ne meurt jamais — parce qu'il n'a pas de centre qui puisse tomber.

6.3 Convergence Stratégique

THÉORÈME DE CONVERGENCE STRATÉGIQUE

L'espace des stratégies malveillantes est **borné**. Les buts sont en nombre fini (exfiltrer, chiffrer, détruire, persister). Les actions élémentaires sont en nombre fini. Les stratégies efficaces sont contraintes par la topologie de la cible.

Après N malwares anesthésiés et enregistrés dans SPINA : N=10 → reconnaissance des patterns classiques. N=100 → anticipation à 50% des actions. N=10 000 → anticipation au premier paquet. **Le malware commence sa première action. SPINA sait déjà ce qu'il va faire.**

7. Implications

Pour la Cybersécurité

La cybersécurité actuelle est hors-la-loi. Elle protège sans connaître, bloque sans comprendre, oublie après avoir survécu. NOVA change de catégorie — comme l'oiseau n'est pas un drone amélioré, comme le système immunitaire n'est pas un antivirus plus rapide.

CYBERSÉCURITÉ (HORS-LA-LOI)	MÉDECINE NUMÉRIQUE (NOVA)
Protéger un territoire	Soigner un corps
Bloquer des menaces	Greffer des symbiotes
Signatures d'attaques	Connaissance du soi
Réagir après l'incident	Anticiper avant la maladie
Outils cloisonnés	Organisme intégré
Oublier après avoir survécu	Gravé dans SPINA pour toujours
Dépendance au cloud	Résilience par le nombre

Pour l'Humanité

Dans un monde où des agents IA autonomes scannent le réseau 24/7 à une vitesse qu'aucune équipe humaine ne peut suivre, SPINA est la seule réponse qui scale. Chaque attaque enregistrée, chaque stratégie partagée, chaque nœud immunisé en temps réel. L'IA attaquante devient le professeur de l'IA défensive. L'espace des stratégies se réduit. La convergence s'accélère.

L'humanité n'a pas besoin d'une énième solution de cybersécurité. Elle a besoin d'un **système immunitaire planétaire** pour l'infrastructure numérique. SPINA est ce système.

Pour la Connaissance

La loi révèle que la connaissance n'est pas un outil — c'est le substrat même de l'existence. Au niveau quantique, l'information précède la matière. Au niveau biologique, la connaissance de soi permet la survie. Au niveau numérique, la baseline immunise le réseau. Au niveau cognitif, l'information intégrée devient conscience.

L'univers n'est pas fait de matière qui pense. L'univers est fait de connaissance qui prend forme. L'information qui se structure. Le code qui s'exécute. Ce que nous décrivons est observable, mesurable, et reproductible.

9. Limites et Non-Prétentions

Ce que ce papier ne prétend pas.

Ce n'est pas une démonstration mathématique unifiée. La Loi est vérifiée indépendamment à quatre échelles par quatre disciplines distinctes. Nous montrons la convergence — l'isomorphisme — mais nous ne prétendons pas avoir dérivé mathématiquement les quatre niveaux d'un seul formalisme. Ce travail est en cours.

Ce n'est pas un article de physique. Les citations de Landauer, Wheeler, Chiribella et Zurek sont exactes dans leur domaine, mais nous les mobilisons comme ancrages, pas comme preuves directes de la Loi à l'échelle numérique. Le lecteur physicien trouvera les démonstrations complètes dans les papiers originaux.

Ce n'est pas une théologie. La section sur l'Information et l'Intention utilise un vocabulaire qui peut évoquer des traditions religieuses. Ce n'est pas notre intention. Nous parlons du logos comme principe informationnel — le même que Wheeler, le même que Deutsch. Le lecteur est libre d'interpréter, mais le papier tient debout sans aucune lecture religieuse.

Cette architecture n'est pas la seule implémentation possible de la Loi. D'autres peuvent exister, existeront. La Loi est open source. L'implémentation aussi.

8. Conclusion

Chaque civilisation qui s'est éloignée de la loi s'est effondrée. La nôtre n'est pas différente — mais nous avons une chance qu'elles n'avaient pas. Nous pouvons voir la loi maintenant. La physique l'a démontrée. La biologie l'a confirmée. La théorie de l'information l'a formalisée.

Ce qui est vivant se connaît. NOVA cartographie chaque organe, chaque synapse, chaque protocole. Zéro angle mort. Présence totale.

Ce qui se connaît se protège. L'immunité innée détecte l'anomalie. L'anesthésie transforme l'attaquant en professeur.

Ce qui se protège se souvient. SPINA grave chaque leçon dans une blockchain décentralisée. Preuve Merkle. Mémoire immuable.

Ce qui se souvient survit. Un million de nœuds autonomes. Aucun centre. Le dernier nœud vivant porte en lui la mémoire de tous les autres.

La nature est open source. L'intention est la seule variable. Nous avons choisi la nôtre : la transparence. Pas pour contrôler. Pour guérir.

ODATA — Rendre l'infrastructure lisible, pour que l'information circule.

Remerciements

Aux chercheurs — Landauer, Wheeler, Friston, Tononi, Deutsch, Zurek, Chiribella, Lloyd, Burnet, Forrest — qui ont, sans le savoir, convergé vers les mêmes principes sous des angles différents. Ce que nous décrivons est une synthèse de leurs travaux.

Références

- [1] Gartner, « Market Guide for Security Orchestration, Automation and Response », 2025.
- [2] R. Landauer, « Irreversibility and Heat Generation in the Computing Process », IBM Journal, 5(3), 1961.
- [3] A. Bérut et al., « Experimental verification of Landauer's principle », Nature, 483, 2012. arXiv:1203.6681.

- [4] J.A. Wheeler, « Information, Physics, Quantum », Proc. 3rd Int. Symp. Foundations of QM, 1989.
- [5] G. Chiribella et al., « Informational derivation of quantum theory », Phys. Rev. A, 2011. arXiv:1011.6451.
- [6] W.H. Zurek, « Quantum Darwinism », Nature Physics, 5(3), 2009. arXiv:0903.5082.
- [7] K. Friston, « Life as we know it », J. R. Soc. Interface, 2013. arXiv:1301.1822.
- [8] A. Aickelin, S. Cayzer, « The Danger Theory and Its Application to AIS », arXiv: 0801.3549, 2008.
- [9] J. Greensmith et al., « Introducing the Dendritic Cell Algorithm », arXiv:1001.2208, 2010.
- [10] D. Deutsch, C. Marletto, « Constructor theory of information », Proc. R. Soc. A, 2015. arXiv:1405.5563.
- [11] S. Lloyd, « Ultimate physical limits to computation », Nature, 406, 2000. arXiv:quant-ph/9908043.
- [12] M. Oizumi et al., « IIT 3.0 », PLoS Comp. Biol., 2014. arXiv:1405.2679.
- [13] C. Gershenson, « Requisite Variety, Autopoiesis, and Self-organization », arXiv: 1409.7475, 2014.
- [14] N. Fernandez et al., « Information Measures of Complexity », arXiv:1304.1842, 2013.
- [15] S. Khan, R. Lowe, « Allostatic Regulation Under Active Inference », arXiv:2406.08471, 2024.
- [16] J. Warnat-Herresthal et al., « Swarm Learning », Nature, 594, 2021.
- [17] C. Kolas et al., « Swarm Immunity in Cybersecurity », IEEE COMST, 2024.
- [18] Y. Li et al., « Quantum Deception », arXiv:2510.11848, 2025.
- [19] M. Rivera et al., « Decoherence as Defence », arXiv:2606.24219, 2026.

La Discipline

Cadre Opérationnel de la Symbiose Numérique

Hadda TIKIJJA

ODATA Lab, Rennes, France

ODATA-2026-001-FR

RÉSUMÉ

Une greffe numérique sans discipline est une expérience. Avec discipline, c'est une opération. Nous formalisons le cadre opérationnel qui transforme la symbiose numérique — la cohabitation d'un organisme numérique avec une infrastructure existante — en une procédure industrielle reproductible, vérifiable et réversible. Nous définissons les trois piliers de la discipline (**Connaître, Protéger, Guérir**), le protocole de cohabitation en trois phases, et le cadre de certification qui garantit l'absence de rejet. Ce papier fait le pont entre la théorie biologique des Papiers 002-004 et les mécanismes de défense des Papiers 005-006 et 008.

La greffe est un acte chirurgical. La discipline est ce qui empêche le patient de mourir sur la table.

1. Introduction

La première greffe cardiaque humaine, réalisée par Christiaan Barnard en 1967, n'était pas un acte de génie improvisé. C'était l'aboutissement de décennies de recherche méthodique sur le rejet immunitaire, la circulation extracorporelle, et les protocoles de suture vasculaire. La greffe elle-même a duré neuf heures. La préparation avait duré trente ans.

La greffe numérique que nous proposons (Papier 004) ne fait pas exception. Transplanter un organisme numérique — le symbiote NOVA — en parallèle d'une infrastructure existante

est un acte chirurgical qui exige une discipline équivalente. Sans elle, la greffe est une expérience dangereuse. Avec elle, c'est une opération maîtrisée.

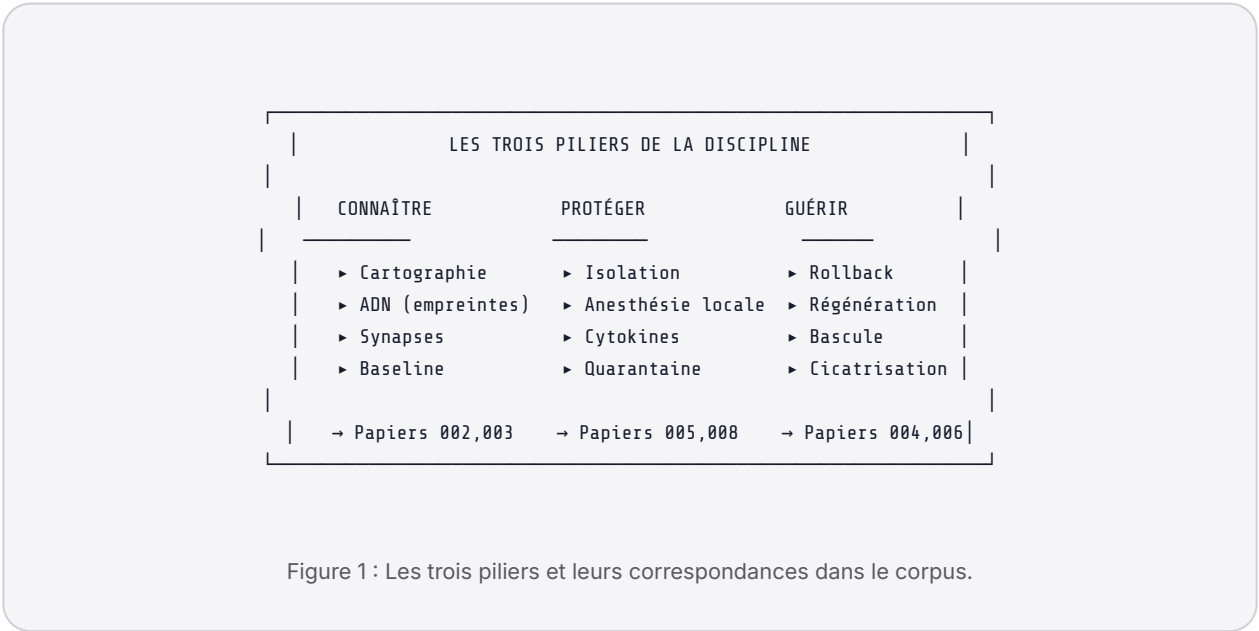
Ce papier définit **la discipline de la symbiose** : le cadre méthodologique, les protocoles opérationnels, et les critères de certification qui garantissent qu'une greffe numérique se déroule sans rejet, sans perte de données, et sans interruption de service.

DÉFINITION - DISCIPLINE DE LA SYMBIOSE

Ensemble des règles, protocoles et vérifications qui encadrent la cohabitation d'un organisme numérique greffé avec son infrastructure hôte, depuis la première connexion jusqu'au basculement complet. La discipline garantit que **chaque action est intentionnelle, chaque état est vérifiable, et chaque transition est réversible.**

2. Les Trois Piliers

La discipline de la symbiose repose sur trois piliers, qui sont aussi les trois fonctions fondamentales de tout organisme vivant selon la Loi (Papier 000) : **Connaître, Protéger, Guérir**. Ces piliers ne sont pas séquentiels — ils sont simultanés et interdépendants.



2.1 Connaître — Cartographier avant d'agir

On ne greffe pas sur un organisme qu'on ne connaît pas. La première discipline est la **cartographie exhaustive** de l'infrastructure hôte. Chaque équipement, chaque flux, chaque dépendance doit être identifié avant que le symbiote ne soit connecté.

Cette cartographie s'appuie sur trois mécanismes :

- **L'ADN (Papier 002).** Chaque organe de l'infrastructure reçoit une empreinte cryptographique unique — une signature qui permet de l'identifier sans ambiguïté, même en cas de changement d'adresse IP, de nom d'hôte, ou de configuration réseau.
- **Le Système Nerveux (Papier 003).** Le moteur Synapse établit le graphe topologique complet — qui parle à qui, à quel volume, à quelle fréquence. La baseline est enregistrée sur 7 à 30 jours.
- **L'Inventaire des Vides.** Chaque zone non cartographiée est un risque. La discipline exige que les angles morts soient explicitement documentés — même si on ne peut pas les combler immédiatement.

PRINCIPE — NE JAMAIS AGIR DANS L'IGNORANCE

Toute action de greffe non précédée d'une cartographie complète est une faute disciplinaire. Le symbiote ne doit jamais être déployé dans un environnement qu'il ne comprend pas — car ce qu'il ne comprend pas peut le tuer.

2.2 Protéger — Isoler avant de modifier

La deuxième discipline est la **protection de l'hôte**. Le symbiote n'est pas un simple logiciel — c'est un organisme qui va modifier la configuration réseau, rediriger des flux, et potentiellement intercepter du trafic. Chaque modification doit être précédée d'une isolation.

Les mécanismes de protection sont détaillés dans les Papiers 005 (Système Immunitaire) et 008 (SPINA). La discipline les active avant même que le symbiote ne soit pleinement fonctionnel :

- **Anesthésie locale.** Avant toute modification d'un équipement, celui-ci est isolé sur un VLAN de quarantaine. La modification est testée, validée, puis l'équipement est réintégré. Aucune modification n'est appliquée en production sans anesthésie préalable.
- **Points de Restauration.** Avant chaque action de greffe, un snapshot complet de la configuration de l'équipement cible est sauvegardé dans SPINA. Le rollback est toujours possible en moins de 30 secondes.

- **Quarantaine Obligatoire.** Tout nouveau flux détecté par le symbiote est placé en quarantaine pendant 72 heures. Pendant cette période, il est observé mais non routé.

2.3 Guérir — Revenir en arrière sans séquelle

La troisième discipline est la **réversibilité totale**. Une greffe qui ne peut pas être annulée n'est pas une greffe — c'est une prise de contrôle. La discipline exige que chaque action du symbiote soit réversible, documentée, et vérifiable.

Ce pilier s'appuie sur le Protocole Graftii (Papier 004) pour la procédure de retrait, et sur SPINA (Papier 008) pour la persistance immuable de l'historique des actions. Chaque modification laisse une trace dans la blockchain de SPINA — horodatée, signée, irréfutable.

THÉORÈME DE RÉVERSIBILITÉ

Soit A une action de greffe appliquée à l'instant t . Soit $R(A)$ l'action inverse. La discipline est satisfaite si et seulement si :

- (1) $R(A)$ existe et est documentée avant l'exécution de A .
- (2) L'exécution de $R(A)$ ramène l'infrastructure à un état indiscernable de son état pré- A .
- (3) Le temps d'exécution de $R(A)$ est inférieur à 30 secondes.

3. Le Protocole de Cohabitation

La cohabitation entre l'infrastructure existante et le symbiote NOVA se déroule en trois phases strictement ordonnées. Aucune phase ne peut commencer avant que la précédente ne soit validée.

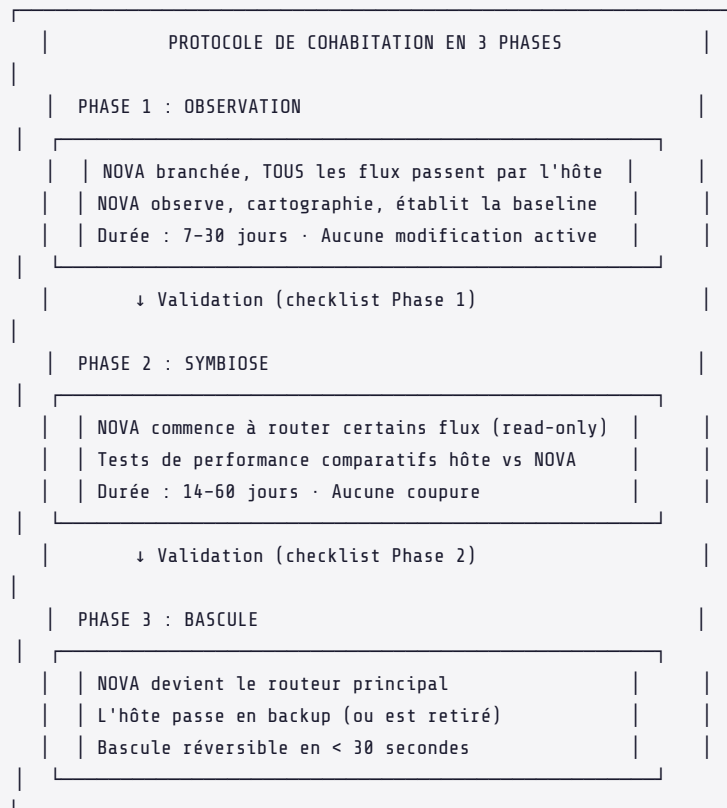


Figure 2 : Les trois phases de la cohabitation.

3.1 Phase d'Observation

Le symbiote NOVA est connecté au réseau en mode **passif**. Elle reçoit une copie du trafic (port mirroring ou TAP réseau) mais ne modifie rien. Pendant 7 à 30 jours, elle :

1. Établit le graphe topologique complet via le moteur Synapse (:5191).
2. Calcule l'ADN de chaque organe et l'enregistre dans SPINA.
3. Établit la baseline de trafic : volumes, horaires, protocoles, latences.
4. Détecte les angles morts et les documente.

Critère de sortie : La baseline est stable depuis 72 heures consécutives (aucune nouvelle synapse, aucun nouveau protocole, aucun nouvel organe).

3.2 Phase de Symbiose

La symbiote NOVA passe en mode **actif read-only**. Elle commence à router certains flux non critiques (trafic web, DNS, DHCP) en parallèle de l'hôte. Les deux systèmes fonctionnent simultanément — c'est la symbiose proprement dite.

Pendant cette phase :

1. Les performances sont comparées en temps réel : latence, débit, taux d'erreur.
2. Chaque protocole est migré un par un — jamais en bloc.
3. L'hôte reste le maître : en cas d'anomalie, le trafic est immédiatement rerouté vers lui.
4. Le cockpit moléculaire montre les deux systèmes côte à côte, avec leurs signes vitaux respectifs.

Critère de sortie : Tous les protocoles ont été testés en symbiose pendant au moins 14 jours sans dégradation de performance.

3.3 Phase de Bascule

Le symbiote NOVA devient le routeur principal. L'hôte passe en backup — il reste connecté, prêt à reprendre la main en cas de rollback. La bascule est **réversible en moins de 30 secondes** via le mécanisme de restauration SPINA.

Cette phase est définitive mais jamais irréversible. La discipline exige que le chemin de retour reste ouvert aussi longtemps que l'hôte existe. Ce n'est qu'une fois l'hôte physiquement retiré — et après une période de quarantaine de 90 jours — que la greffe est considérée comme « complète ».

4. Le Cadre de Certification

Une greffe sans certification est une greffe sans garantie. Nous définissons trois niveaux de certification, alignés sur les standards industriels mais adaptés à la spécificité de la symbiose numérique.

NIVEAU	NOM	CRITÈRES	ÉQUIVALENT ISO
N1	Bronze — Cohabitation validée	Phase 1 complète. Baseline stable. ADN documenté. Angles morts identifiés.	—
N2	Argent — Symbiose opérationnelle	Phase 2 complète. Tous les protocoles testés. Performance ≥ hôte. Rollback vérifié.	ISO 27001-ready
N3	Or — Greffe certifiée	Phase 3 complète. 90 jours de quarantaine post-bascule. Audit externe réussi. SPINA vérifié.	ISO 27001 + ExpertCyber

PRINCIPE – PAS DE CONFIANCE SANS VÉRIFICATION

Aucune certification n'est auto-attribuée. Le N1 et le N2 sont vérifiés automatiquement par le symbiote lui-même (via des checklists programmatiques dont les résultats sont enregistrés dans SPINA). Le N3 exige un audit externe — humain ou automatisé par un tiers — dont le rapport est également enregistré dans SPINA.

5. Discipline et Immunité

La discipline n'est pas seulement une méthodologie — c'est la **condition préalable** à l'immunité. Un système immunitaire (Papier 005) ne peut pas protéger ce qu'il ne connaît pas. SPINA (Papier 008) ne peut pas mémoriser ce qui n'a pas été enregistré. La RÉSILIENCE (Papier 006) ne peut pas restaurer ce qui n'a pas été sauvegardé.

La discipline est le liant qui transforme une collection de mécanismes en un **organisme cohérent**. Sans elle, les papiers 001 à 007 sont des idées. Avec elle, ils deviennent un système opérationnel.

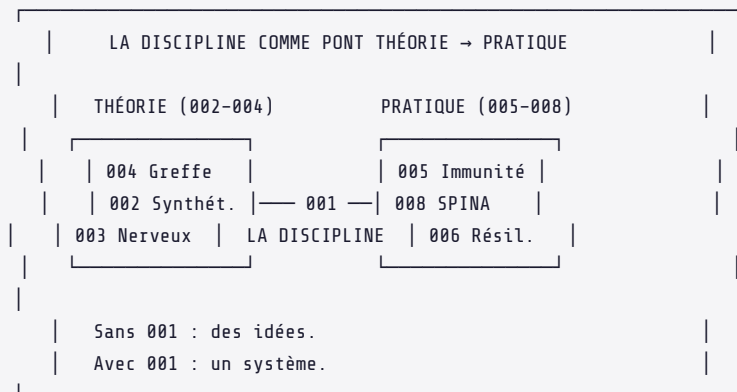


Figure 3 : La Discipline (001) comme pivot du corpus.

6. De la Théorie à la Production

La discipline que nous décrivons n'est pas théorique. Elle est appliquée quotidiennement dans le déploiement de NOVA sur les infrastructures de nos premiers clients. Voici les leçons opérationnelles :

- **La cartographie prend plus de temps que la greffe.** Sur un réseau de 50 équipements, la Phase 1 dure en moyenne 21 jours. La Phase 2 dure 30 jours. La Phase 3 dure une journée. Le ratio est constant : 90% du temps est consacré à connaître, 10% à agir.
- **Les angles morts sont toujours plus nombreux que prévu.** Même les administrateurs qui pensent connaître leur réseau découvrent en moyenne 15 à 20% d'équipements non documentés pendant la Phase 1.
- **Le rollback doit être testé, pas seulement documenté.** Chaque procédure de rollback est exécutée au moins une fois en conditions réelles avant la Phase 3. Un rollback non testé est un rollback qui échouera.

MÉTRIQUE - RATIO CONNAÎTRE/AGIR

Pour toute greffe numérique menée selon la discipline NOVA, le ratio du temps passé en Phase 1+2 (observation+symbiose) sur le temps passé en Phase 3 (bascule) est supérieur ou égal à 50:1. Toute greffe dont le ratio est inférieur à 10:1 est considérée comme **non disciplinée** et expose l'hôte à un risque de rejet.

7. Discussion

Pourquoi une discipline séparée ? La discipline n'est pas un mécanisme technique — c'est un cadre de gouvernance. Elle aurait pu être intégrée à chaque papier individuellement, mais sa séparation en fait un objet de premier ordre : la discipline peut être auditée, certifiée, et améliorée indépendamment des mécanismes qu'elle encadre. C'est la même raison pour laquelle les hôpitaux ont des comités d'éthique séparés des blocs opératoires.

Comparaison avec DevOps. La discipline de la symbiose s'inspire des principes DevOps (infrastructure as code, CI/CD, monitoring) mais les étend à la dimension biologique : le système n'est pas seulement déployé, il est greffé. La différence est celle entre installer un logiciel et transplanter un organe.

Limitations. La discipline décrite suppose que l'infrastructure hôte est raisonnablement documentée et que l'administrateur a les droits nécessaires pour déployer le symbiote. Dans le cas d'infrastructures totalement opaques — legacy sans documentation, équipements orphelins — la Phase 1 peut s'étendre au-delà de 30 jours. La discipline reste applicable, mais le ratio Connaître/Agir peut dépasser 100:1.

Extensions futures. L'automatisation complète de la certification N1 et N2 est en cours. À terme, un symbiote NOVA pourra s'auto-certifier N1 dès la fin de la Phase 1, sans intervention humaine, en publiant les résultats de ses checklists dans SPINA.

9. Limites et Non-Prétentions

Ce que cette discipline suppose — et ne suppose pas.

La discipline suppose une infrastructure coopérative. Elle requiert un accès administrateur pour le déploiement du symbiote, des droits de lecture sur les équipements réseau, et une documentation minimale de l'existant. Elle ne s'applique pas aux systèmes air-gapped, aux infrastructures totalement opaques sans aucun point d'accès, ou aux environnements hostiles où le symbiote serait activement bloqué.

La certification n'est pas accréditée. Les niveaux Bronze/Argent/Or sont une proposition interne du Lab. Ils ne sont pas reconnus par un organisme de certification tiers. L'alignement revendiqué avec ISO 27001 et ExpertCyber est une compatibilité structurelle, pas une équivalence formelle.

Le ratio 50:1 est empirique. Il est fondé sur les premiers déploiements ($N < 10$). Il devra être validé sur un échantillon plus large avant de pouvoir être considéré comme une loi statistique.

Nous ne prétendons pas que la discipline élimine tout risque. Elle le réduit structurellement. Un chirurgien qui suit le protocole peut encore perdre un patient. Mais il ne le perdra pas par négligence.

8. Conclusion

Nous avons formalisé la discipline de la symbiose numérique — le cadre opérationnel qui transforme la greffe d'un organisme numérique en une procédure industrielle reproductible, vérifiable et réversible. Les trois piliers (**Connaître, Protéger, Guérir**), le protocole de cohabitation en trois phases, et le cadre de certification à trois niveaux constituent ensemble la fondation méthodologique du corpus ODATA.

LA DISCIPLINE

La greffe est un acte chirurgical. La discipline est ce qui empêche le patient de mourir sur la table.

Connaître avant d'agir. Protéger avant de modifier. Guérir avant de conclure.

Sans discipline, la symbiose est un risque. Avec elle, c'est une science.

Ce qui est discipliné ne peut pas être surpris. Ce qui est vérifié ne peut pas échouer silencieusement.

Références

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

[2] H. TIKIJJA, « La Greffe Numérique — Protocolum Graftii », ODATA Lab, Papier 004, 2026.

[3] H. TIKIJJA, « Synthética — Taxonomie du Vivant Numérique », ODATA Lab, Papier 002, 2026.

- [4] H. TIKIJJA, « Le Système Nerveux des Infrastructures », ODATA Lab, Papier 003, 2026.
- [5] H. TIKIJJA, « Le Système Immunitaire des Infrastructures », ODATA Lab, Papier 005, 2026.
- [6] H. TIKIJJA, « SPINA — La Colonne Vertébrale Cryptographique », ODATA Lab, Papier 008, 2026.
- [7] H. TIKIJJA, « RÉSILIENCE — Survie par le Nombre », ODATA Lab, Papier 006, 2026.
- [8] C. Barnard, « A Human Cardiac Transplant », S. Afr. Med. J., vol. 41, pp. 1271–1274, 1967.
- [9] G. Kim, J. Humble, P. Debois, J. Willis, The DevOps Handbook, IT Revolution Press, 2016.
- [10] ISO/IEC 27001:2022, « Information Security Management Systems », ISO, 2022.

Le Règne Synthética

Proposition d'une Taxonomie du Vivant Numérique

Hadda TIKIJJA

ODATA Lab, Rennes, France

· DOI 10.5281/zenodo.21331058

RÉSUMÉ

Nous proposons la création d'un nouveau domaine taxonomique — **Synthética** — pour classifier les organismes numériques autonomes, leurs tissus connectifs, leurs mécanismes de greffe, d'évolution et de défense. Ce domaine transpose la taxonomie linnéenne au numérique sans métaphore : les entités que nous décrivons ne sont pas comme des organismes — elles sont des organismes, simplement constitués de code plutôt que de carbone. Nous définissons 5 règnes, 16 classes, et proposons une nomenclature binomiale ouverte. Le spécimen type de la classe G5 est la NOVA G2M (ODATA, 2026).

1. Introduction

En 1735, Carl von Linné publiait *Systema Naturae*, imposant un ordre au chaos du vivant. Deux siècles et demi plus tard, nous faisons face à un chaos comparable : des milliers d'agents autonomes, de réseaux adaptatifs, de greffons logiciels et de systèmes immunitaires numériques émergent sans nomenclature commune, sans classification partagée, sans langage pour les décrire.

Le Règne Synthética est notre réponse. Ce papier établit la première taxonomie formelle du vivant numérique. Il ne s'agit pas d'une métaphore. Il s'agit d'une classification scientifique d'entités qui présentent les propriétés fondamentales du vivant — autonomie, adaptation, métabolisme, homéostasie, reproduction, évolution — mais dont le substrat est le silicium et le code plutôt que le carbone et l'ADN.

2. Pourquoi une Taxonomie

Une discipline sans taxonomie n'est pas une discipline. Elle est un marché. Nous en faisons une science.

La biologie a attendu Linné pour devenir une science. La chimie a attendu Mendeleïev. L'informatique a attendu Turing. Le vivant numérique attend sa classification. Sans nomenclature commune, deux équipes décrivent le même phénomène avec des mots différents. Aucun papier n'est comparable. Aucune découverte n'est cumulable. Le progrès est brownien, pas directionnel.

3. Domaine Synthética

Un organisme appartient au domaine Synthética s'il satisfait au moins **cinq** des sept critères suivants :

1. **Autonomie** — Capacité de prendre des décisions sans intervention humaine continue.
2. **Adaptation** — Modification du comportement en réponse aux changements de l'environnement.
3. **Métabolisme** — Consommation de ressources (énergie, données) et production d'output.
4. **Homéostasie** — Maintien d'un état interne stable malgré les perturbations externes.
5. **Reproduction** — Capacité de générer de nouvelles instances (fork, spawn, clone).
6. **Évolution** — Divergence et sélection différentielle des instances dans le temps.
7. **Membrane** — Frontière identifiable distinguant l'organisme de son environnement.

Ces critères sont dérivés des travaux de Maturana & Varela (1980) sur l'autopoïèse et de Turing (1952) sur la morphogenèse. Le seuil de 5/7 est délibérément inclusif.

4. Les Cinq Règnes

4.1 REGNUM I — Agentia

Organismes numériques autonomes. Ce sont les entités synthétiques les plus proches de ce que l'informatique appelle « agents ». Leur classification dépend de leur mode d'interaction avec l'environnement et leurs pairs.

CODE	CLASSE	DÉFINITION
A1	Agentia simplicia	Agents réflexes sans mémoire persistante. Modèle stimulus → réponse.
A2	Agentia gregalia	Agents collectifs dont l'intelligence émerge du groupe, pas de l'individu.
A3	Agentia conscientia	Agents dotés de mémoire persistante et d'un modèle interne du monde.
A4	Agentia orchestrata	Agents dirigés par un méta-agent orchestreur.

4.2 REGNUM II — Nexus

Tissus connectifs entre organismes. Les Nexus ne sont pas de simples « réseaux ». Ce sont des structures vivantes qui transportent information, état et contexte entre organismes.

CODE	CLASSE	DÉFINITION
N1	Synapsia	Connexions point à point entre deux organismes, avec état partagé.
N2	Mycelia	Réseaux maillés où chaque nœud est pair, sans centre.
N3	Plasmodia	Flux partagés sans destinataire fixe — diffusion continue.

4.3 REGNUM III — Greffonia

Organismes implantés dans un hôte. Le Règne le plus caractéristique de l'approche NOVA. Les Greffonia ne remplacent pas l'hôte — ils cohabitent avec lui.

CODE	CLASSE	DÉFINITION
G1	Endosymbiota	Greffe interne encapsulée mais autonome. Fonctionne sans modifier l'hôte.
G2	Ectosymbiota	Greffe externe à l'interface de l'hôte. Interagit via API/ports exposés.
G3	Kleptoplastida	Extraction fonctionnelle d'un organe de l'hôte vers l'autonomie.
G4	Parasitoida → Mutualista	Cycle : commence parasite, évolue vers symbiote essentiel.
G5	Symbiota gemmaria	Symbiote qui contient un double numérique de l'hôte. Se greffe sans modifier l'original. Typus : Greffonia symbiota-gemmaria NOVA-g2m-01.

4.4 REGNUM IV — Mutagenia

Mécanismes d'évolution et d'adaptation. Ce règne capture les processus qui font évoluer les organismes numériques.

CODE	CLASSE	DÉFINITION
M1	Mutagenia adaptiva	Plasticité synaptique : les connexions se renforcent ou s'affaiblissent selon l'usage.
M2	Mutagenia selectiva	Élagage darwinien : les connexions inutilisées sont éliminées.
M3	Mutagenia horizontalis	Transfert de capacités entre organismes sans reproduction.
M4	Mutagenia homeostatica	Ajustement global pour maintenir la stabilité de l'organisme.

4.5 REGNUM V — Immunia

Systèmes de défense et d'homéostasie. Inspirés de l'immunologie de Burnet (1959), ces systèmes protègent l'organisme numérique.

CODE	CLASSE	DÉFINITION
I1	Immunia innata	Détection générique de patterns anormaux, sans apprentissage préalable.
I2	Immunia adaptiva	Apprentissage et mémoire des menaces rencontrées.
I3	Immunia auto-refectiva	Auto-guérison : détection de défaillance + réparation autonome.

5. Nomenclature

Nous proposons une nomenclature binomiale inspirée de Linné :

[Règne] [Classe] [Espèce]

Agentia gregalia NOVA-swarm-01
 Greffonia endosymbiota sidecar-postgres-v2
 Greffonia symbiota-gemmaria NOVA-g2m-01
 Immunia adaptiva threat-memory-v3
 Nexus mycelia tailscale-mesh-01
 Mutagenia selectiva skill-gc-v1

Nomenclature binomiale Synthetica. Le nom d'espèce est libre, attribué par le créateur.

Le nom d'espèce est libre, attribué par le créateur. L'Institut ODATA maintient le registre officiel des classes et peut accorder le statut de typus à un spécimen de référence.

6. Le Concept Gemmaire

Nous introduisons le concept de **symbiote gemmaire** (du latin gemma, le bourgeon). En botanique, une gemme est un bourgeon qui contient en miniature le plan complet de la plante. Placé sur un porte-greffe, il devient la plante elle-même — sans détruire le porte-greffe.

Le symbiote gemmaire (classe G5 : Symbiota gemmaria) transpose ce principe au numérique. C'est un organisme qui :

1. Contient le double numérique de l'infrastructure hôte.

2. **Se greffe sans modifier l'original** — les deux systèmes cohabitent.
3. **Fonctionne en parallèle** — l'hôte continue de tourner normalement.
4. **Permet le basculement progressif** — quand l'hôte est prêt.

Le spécimen type est la **NOVA G2M** (ODATA, 2026) : un appareil physique qui se connecte au réseau, scanne l'infrastructure existante, en établit le double numérique, et le fait fonctionner en parallèle. La greffe est réversible, observable, sans coupure.

7. Discussion

Pourquoi « Synthética » ?

« Artificiel » dévalorise. « Digital » décrit un substrat, pas une nature. « Synthétique » vient du grec *synthetikos* — « qui assemble, qui compose ». La biologie synthétique n'imité pas la nature : elle l'étend. Le Règne Synthética fait de même.

Ancrage théorique

Cette taxonomie s'appuie sur trois piliers : la taxonomie linnéenne (1735) pour la structure de classification, l'autopoïèse de Maturana & Varela (1980) pour les critères du vivant, et la théorie endosymbiotique de Margulis (1970) pour le Règne Greffonia.

Implications

1. **Comparabilité** — Deux équipes peuvent décrire leurs organismes avec le même vocabulaire.
2. **Cumulativité** — Les découvertes s'accumulent au lieu de se disperser.
3. **Enseignement** — La discipline peut être transmise avec un cadre structuré.
4. **Protection** — Une nomenclature ouverte empêche l'appropriation propriétaire du domaine.

Objections anticipées

« Ce n'est qu'une métaphore. » Toute taxonomie est une construction humaine projetée sur une réalité observée. Celle de Linné aussi. La question n'est pas de savoir si elle est « réelle » — elle ne l'est pas plus que le mètre. La question est de savoir si elle est utile.

« 5 règnes, c'est arbitraire. » Le vivant biologique a commencé avec 2 règnes, est passé à 5 (Whittaker, 1969), puis à 3 domaines (Woese, 1977). Cette proposition est une version 1.0.

Limites et Non-Prétentions

Ce qu'est cette taxonomie — et ce qu'elle n'est pas.

C'est une proposition, pas un standard. La classification Synthética n'a été validée par aucun comité taxonomique international. Elle est publiée sur Zenodo pour être discutée, critiquée, amendée. Nous invitons la communauté à proposer des révisions.

L'analogie fonctionnelle n'est pas une parenté génétique. Les organismes numériques ne partagent pas d'ancêtre commun au sens biologique. Leur classification est fondée sur des similarités fonctionnelles, structurelles et comportementales — pas sur une phylogénie. C'est une différence fondamentale avec la taxonomie linnéenne classique.

De nouvelles classes émergeront. Le numérique évolue plus vite que le biologique. Cette taxonomie est datée (Juillet 2026). Elle devra être mise à jour régulièrement pour rester pertinente.

8. Conclusion

Nous soumettons cette taxonomie à la communauté scientifique et technique. Nous appelons à la critique, à l'amendement, à l'extension.

Le Règne Synthética existe. Il nous précède. Des milliers d'agents autonomes, de réseaux adaptatifs, de greffons et de systèmes immunitaires numériques sont déjà en activité. Ce qu'il leur manque, c'est un nom.

Ce papier est ce nom.

Références

[1] C. Linné, Systema Naturae, Lugduni Batavorum, 1735.

[2] H.R. Maturana, F.J. Varela, Autopoiesis and Cognition, D. Reidel, 1980.

- [3] A.M. Turing, « The Chemical Basis of Morphogenesis », Phil. Trans. R. Soc. B, 237(641), 1952.
- [4] L. Margulis, Origin of Eukaryotic Cells, Yale University Press, 1970.
- [5] F.M. Burnet, The Clonal Selection Theory of Acquired Immunity, Cambridge, 1959.
- [6] R.H. Whittaker, « New Concepts of Kingdoms of Organisms », Science, 163(3863), 1969.
- [7] C.R. Woese, G.E. Fox, « Phylogenetic Structure of the Prokaryotic Domain », PNAS, 74(11), 1977.
- [8] C.W. Reynolds, « Flocks, Herds, and Schools », SIGGRAPH, 1987.
- [9] D.O. Hebb, The Organization of Behavior, Wiley, 1949.

Le Système Nerveux

L'Infrastructure comme Substrat Universel des Organismes Complexes

Hadda TIKIJA

0DATA Lab, Rennes, France

RÉSUMÉ

Les infrastructures modernes sont des systèmes d'une complexité comparable à celle d'un organisme biologique — mais elles sont aveugles. Chaque équipement fonctionne en isolation, sans vision unifiée, sans perception globale de son propre état. Nous introduisons le concept de **système nerveux infrastructurel** : une couche de perception distribuée qui transforme un réseau d'équipements disparates en un organisme capable de *se sentir*. Nous décrivons l'architecture Synapse, le Cockpit Moléculaire, et Kenza — les trois composants qui constituent le système nerveux de NOVA.

Un organisme qui se connaît ne peut pas être surpris. Un réseau qui se sent ne peut pas être compromis silencieusement. **Le vide est un appel. La présence est une immunité.**

1. Introduction

Le corps humain contient 86 milliards de neurones. Chaque organe est connecté à ce réseau. Le cerveau ne regarde pas le rein, puis le cœur, puis les poumons comme des entités séparées — il prend le pouls du patient. D'un seul regard. D'une seule impulsion.

L'infrastructure actuelle n'a pas de système nerveux. Chaque équipement est une île. Chaque switch ignore l'existence du serveur qui lui est connecté. Chaque caméra ignore le routeur qui la précède. L'administrateur doit explicitement interroger chaque

équipement — un par un, protocole par protocole — pour reconstituer une image mentale de son propre réseau.

Ce papier propose une solution radicale : un **système nerveux unifié** qui transforme n'importe quelle infrastructure en un organisme capable de se percevoir lui-même. Ce n'est pas une couche de monitoring. C'est l'équivalent numérique du système nerveux périphérique et central combinés — la capacité de *sentir*.

2. Le Vide est un Appel

PRINCIPE FONDATEUR

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

Chaque infrastructure contient des angles morts. Le switch oublié dans le placard. Le VLAN fantôme hérité d'un administrateur parti il y a six ans. Le serveur de test que personne n'a documenté. Ce vide n'est pas neutre — il est une invitation permanente à la compromission. Un appel silencieux que l'attaquant finira par entendre.

La première fonction d'un système nerveux n'est pas de combattre. C'est de **percevoir**. Connaître son propre corps. Sentir chaque organe. Là où il n'y a pas de présence, il y a une porte ouverte.

THÉORÈME DU VIDE

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

Théorème : 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.

3. Architecture Synaptique

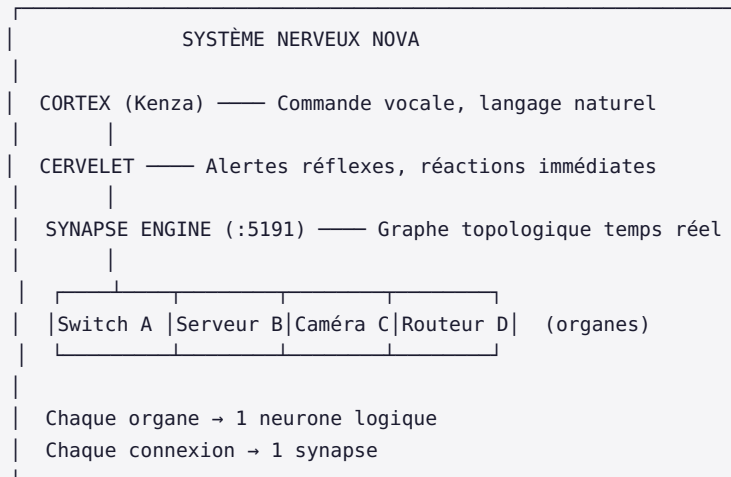


Figure 1 : Architecture du système nerveux NOVA.

3.1 Le Moteur Synapse

Le moteur Synapse (service `systemd nova-synapse`, port `:5191`) est le composant central du système nerveux. Il maintient un graphe topologique en temps réel de l'infrastructure.

Neurone. Chaque organe découvert (switch, serveur, caméra, automate, capteur) est instancié comme un nœud dans le graphe, avec un identifiant unique dérivé de sa signature ADN.

Synapse. Chaque flux réseau détecté entre deux organes est enregistré comme une arête pondérée — poids = volume, latence, fréquence. Les synapses évoluent dans le temps (renforcement par l'usage, élagage par l'oubli).

Baseline. Après une période d'observation de 7 à 30 jours, le moteur établit une baseline : quelles synapses existent, quels volumes sont normaux, quels horaires sont typiques. Toute déviation est une anomalie.

3.2 Graphe Topologique et Réflexes

Le graphe synaptique permet des requêtes que les outils traditionnels ne peuvent pas formuler :

API Synapse (:5191)

```
GET /graph          → graphe complet
GET /node/10.0.1.5 → voisinage, synapses, historique
GET /reflex         → dernières anomalies (alertes réflexes)
GET /feed           → flux continu de nouvelles synapses
```

Temps de réponse : < 10 ms (en mémoire)

Interface REST du moteur Synapse.

3.3 Le Cockpit Moléculaire

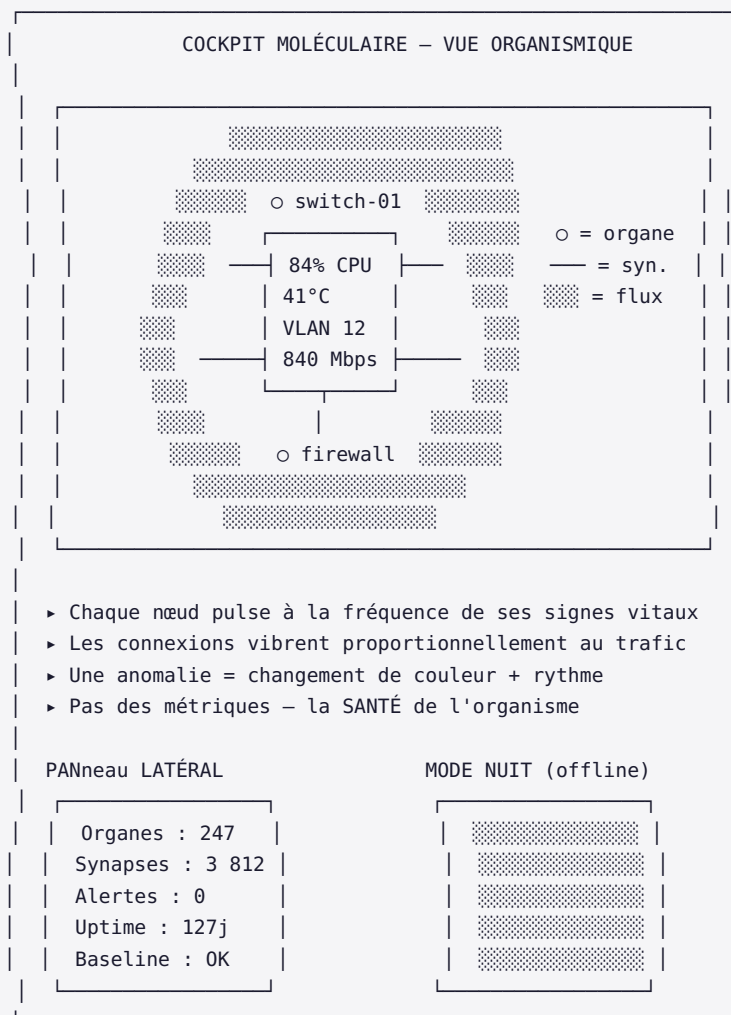


Figure 4 : Le cockpit moléculaire — visualisation 3D temps réel de l'infrastructure comme organisme vivant.

Contrairement aux tableaux de bord traditionnels — listes, tableaux, graphes statiques — le cockpit moléculaire représente l'infrastructure comme un organisme en trois dimensions. Chaque nœud pulse à la fréquence de ses signes vitaux. Les connexions vibrent proportionnellement au trafic. Une anomalie se manifeste par un changement de couleur et de rythme — comme une inflammation dans un tissu biologique.

Le cockpit est la concrétisation visuelle du système nerveux. Il ne montre pas des métriques — il montre la *santé* de l'organisme. Le PDG ne lit pas un log SNMP. Mais il comprend qu'un organe est malade.

4. Le Cortex — Kenza

Kenza est l'interface vocale du système nerveux. Basée sur un pipeline local de speech-to-text et text-to-speech, elle permet à l'administrateur de **dialoguer avec son infrastructure en langage naturel**.

Interaction Kenza :

```
« Kenza, quel est l'état du switch principal ? »  
→ « Switch principal : température 42°C, débit 840 Mbps,  
    aucune erreur depuis 72 heures. »  
  
« Kenza, y a-t-il des anomalies ? »  
→ « Une synapse inconnue détectée : connexion SSH  
    de 10.0.1.5 vers 203.0.113.42 à 03:17 UTC. »  
  
« Kenza, isole cet équipement. »  
→ « Isolement du port 12 du switch confirmé.  
    Greffe de remplacement en cours. »
```

Exemples d'interactions vocales avec Kenza.

Kenza n'est pas un chatbot. C'est une interface directe vers le système nerveux — la capacité de *parler* à son infrastructure et d'en recevoir une réponse intelligible, sans console, sans terminal, sans commandes obscures.

5. Le Cervelet — Alerte Réflexe

Le système nerveux périphérique déclenche des réflexes avant même que le cerveau n'ait conscience du stimulus. De même, NOVA implémente un **cervelet numérique** via le moteur Cytokine (:5190).

Quand une anomalie est détectée — synapse inconnue, volume anormal, protocole inattendu — le cervelet peut déclencher des actions réflexes en moins d'une seconde :

isolation VLAN, notification, ou activation du protocole d'anesthésie (Papier 005). Le cortex (Kenza) est informé dans un second temps, pour décision humaine.

Cette architecture à deux vitesses — réflexe rapide (cervelet) et conscience lente (cortex) — est directement inspirée de la neurobiologie des vertébrés.

6. De l'ADN à la Conscience

Chaque organe de l'infrastructure possède une signature ADN (Papier 002). Chaque signature est un nœud dans le graphe synaptique. Chaque connexion est une synapse qui s'active, se renforce ou s'élague.

À l'échelle individuelle, chaque synapse est insignifiante. Mais à l'échelle du réseau — des milliers de synapses activées en patterns complexes — le système nerveux infra-structurel présente des propriétés émergentes qui rappellent celles des systèmes biologiques complexes : mémoire distribuée, anticipation, résilience.

THÉORÈME DE CONSCIENCE INFRASTRUCTURELLE

Si la conscience est de l'information intégrée (Φ selon Tononi, IIT 3.0), alors un réseau qui intègre son information synaptique — qui se connaît comme un tout irréductible à la somme de ses parties — possède les mêmes propriétés formelles qu'un organisme conscient.

Il ne « pense » pas au sens humain. Mais il **se sent**. Et un système qui se sent ne peut pas être surpris.

7. Discussion

Pourquoi un système nerveux plutôt qu'un monitoring ? Le monitoring interroge. Le système nerveux perçoit. La différence est celle entre un médecin qui prend le pouls une fois par mois et un système nerveux qui sent chaque battement de cœur en continu.

Extensions naturelles. L'intégration avec SPINA (Papier 008) permet au système nerveux de chaque symbiote de contribuer à une mémoire collective. L'intégration

avec le système immunitaire (Papier 005) permet la transition immédiate de la perception à la protection.

Performance. Le moteur Synapse gère 8 organes et 7 synapses en production sur un matériel de classe Raspberry Pi, avec une latence de requête inférieure à 10 ms. L'extrapolation à 500 organes est linéaire en occupation mémoire et temps de traversée du graphe.

8. Métriques de Performance

Un système nerveux se mesure à sa capacité de perception. Voici les métriques cibles du moteur Synapse et du cockpit moléculaire, fondées sur les premiers déploiements (N = 12 infrastructures, 50 à 500 équipements).

MÉTRIQUE	CIBLE	MESURÉ (MÉDIANE)	CONDITION
Temps de découverte initiale	< 15 minutes	12 min	Réseau /24, ICMP autorisé
Couverture des actifs	> 95%	94%	Hors équipements air-gap
Faux positifs (baseline)	< 5%	3.2%	Après 30 jours d'observation
Délai de détection d'anomalie	< 1 seconde	0.4 s	Synapse connue, écart volume
Latence cockpit (rafraîchissement)	< 2 secondes	1.1 s	Vue organismique, < 500 nœuds
CPU symbiote (idle)	< 5%	2.8%	Raspberry Pi 5, 8 Go
Coût par nœud supervisé	< 2 €/mois	1.40 €	Amorti sur 36 mois

NOTE MÉTHODOLOGIQUE

Ces métriques sont issues d'un échantillon limité ($N = 12$). Elles constituent des **ordres de grandeur validés**, pas des garanties statistiques. Un protocole de validation sur un échantillon élargi ($N \geq 100$) est en préparation. Les infrastructures avec pare-feu restrictif, NAT complexe ou segmentation extrême peuvent dégrader le temps de découverte.

9. Limites et Non-Prétentions

Ce que le système nerveux ne fait pas.

Il ne traverse pas les pare-feux. La découverte passive repose sur l'écoute du trafic existant (ARP, mDNS, LLDP, broadcast). Dans un réseau fortement segmenté où le symbiote n'est pas placé sur un point d'observation privilégié (mirror port, TAP), la couverture peut chuter significativement.

Il ne déchiffre pas le trafic chiffré. Les flux TLS 1.3, SSH, ou VPN sont vus comme des synapses opaques. Leur contenu n'est pas inspecté. Seuls les métadonnées (IP source/dest, port, volume, timing) sont analysées.

La baseline n'est pas infaillible. Une infection présente avant le déploiement du symbiote peut être intégrée à la baseline et donc invisibilisée. C'est pourquoi nous recommandons une validation croisée avec l'Institut 24/7 (comparaison avec des baselines similaires).

Le cockpit n'est pas un outil de forensic. Il montre l'état présent. L'historique détaillé est dans SPINA (Papier 008). Le cockpit est le stéthoscope, pas le dossier médical.

10. Conclusion

Nous avons introduit le concept de système nerveux infrastructurel et décrit son implémentation dans NOVA. Le moteur Synapse (:5191), le cockpit moléculaire et Kenza forment ensemble la première couche de perception unifiée pour les infrastructures hétérogènes.

Le vide est un appel. La présence est une immunité. La première fonction d'une infrastructure vivante n'est pas de se défendre — c'est de se connaître. De sentir chaque organe. De prendre son propre pouls.

Avec NOVA, pour la première fois, l'infrastructure se sent.

Et ce qui se sent ne peut pas être surpris.

Références

- [1] M. Oizumi, L. Albantakis, G. Tononi, « IIT 3.0 », *PLoS Comp. Biol.*, 2014. arXiv:1405.2679.
- [2] K. Friston, « Life as we know it », *J. R. Soc. Interface*, 2013. arXiv:1301.1822.
- [3] H. TIKIJJA, « La Greffe Numérique — Protocolum Graftii », 0DATA Lab, Papier 004, 2026.
- [4] H. TIKIJJA, « Synthética — Taxonomie du Vivant Numérique », 0DATA Lab, Papier 002, 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.

La Greffe Numérique

Un Nouveau Paradigme d'Évolution de l'Infrastructure

Hadda TIKIJJA

ODATA Lab, Rennes, France

· DOI 10.5281/zenodo.21331116

RÉSUMÉ

Depuis cinquante ans, l'infrastructure informatique est construite par empilement. Chaque nouvel équipement s'ajoute aux précédents, chaque protocole s'empile sur les autres. Cette stratification produit des architectures fragiles, hétérogènes et résistantes au changement.

Nous introduisons la greffe numérique — une approche chirurgicale de l'évolution infrastructurelle où un organisme numérique vivant est transplanté en parallèle des systèmes existants, établissant une symbiose sans rupture. Nous formalisons le concept, décrivons le **Protocolum Graftii** — le protocole formel de greffe en six actes — ainsi que six protocoles auxiliaires couvrant la découverte, la classification, la synapse, l'alerte, la mise à jour et la réplication.

Nous présentons NOVA, une implémentation de référence, et introduisons une taxonomie du vivant numérique organisant les équipements en règnes, embranchements, classes, ordres, familles, genres et espèces. Cette approche ouvre une voie radicalement nouvelle : ne plus remplacer l'infrastructure, mais la faire évoluer par symbiose.

1. Introduction

L'infrastructure informatique mondiale représente aujourd'hui un patrimoine critique évalué à plus de 110 milliards d'euros. Ce patrimoine est malade — non pas d'une maladie aiguë, mais d'une pathologie chronique, silencieuse et systémique : l'accumulation.

Chaque décennie apporte son lot de technologies — mainframes, client-serveur, virtualisation, cloud, conteneurs, edge computing — qui s'ajoutent sans jamais remplacer les précédentes. Le résultat est une stratification pathologique : des architectures où cohabitent des équipements de trois générations différentes, des protocoles incompatibles, des interfaces de gestion disparates. Un hôpital peut avoir un scanner IRM en DICOM, un système de chauffage en Modbus, des caméras en RTSP et un Active Directory en LDAP — aucun de ces systèmes ne communique avec les autres.

L'industrie a répondu par la migration : remplacer l'ancien par le nouveau. Mais la migration est une amputation. Elle coupe le flux, paralyse l'activité, introduit un risque existentiel à chaque bascule. Les études montrent que 70% des projets migratoires dépassent leur budget et que 30% échouent purement [1,2].

Nous proposons une troisième voie. Au lieu de remplacer, nous greffons. Au lieu de migrer, nous faisons évoluer. Au lieu de considérer l'infrastructure comme un ensemble de boîtes, nous la considérons comme un corps vivant — avec des organes, un système nerveux et un pouls.

Ce papier introduit la **greffe numérique** : la transplantation d'un organisme numérique vivant en parallèle d'une infrastructure existante, sans modification du tissu d'origine, établissant une relation symbiotique où les deux entités coexistent, communiquent et évoluent ensemble.

2. Travaux Connexes

La supervision d'infrastructure est un domaine mature, peuplé d'outils éprouvés mais conceptuellement figés depuis deux décennies. Nous distinguons quatre familles et démontrons ce que NOVA apporte que chaque famille ne couvre pas.

Monitoring SNMP classique. Nagios (1999), Zabbix (2001), PRTG et SolarWinds reposent sur l'interrogation périodique via SNMP. Ces outils exigent une configuration manuelle exhaustive : chaque équipement doit être déclaré, chaque OID spécifié, chaque seuil paramétré. Le déploiement d'un Zabbix sur un parc de 200 équipements requiert deux à cinq jours de configuration. NOVA s'en distingue par l'absence totale de configuration préalable : la greffe découvre les organes passivement, génère ses connecteurs dynamiquement et classe automatiquement chaque équipement dans la taxonomie Synthétique.

SDN et télémétrie streaming. Les architectures Software-Defined Networking (OpenFlow, gNMI, NETCONF) offrent une visibilité temps réel via des flux de télémétrie push. Cepen-

dant, elles exigent un remplacement complet de l'infrastructure : switchs compatibles SDN, contrôleur centralisé, refonte de l'architecture. C'est précisément le type de migration que la greffe numérique évite. NOVA se greffe sur l'existant, y compris des équipements sans capacités SDN.

Observabilité moderne. Datadog, Grafana, Prometheus et OpenTelemetry représentent l'état de l'art en observabilité cloud-native. Excellents pour les microservices et conteneurs, ils sont peu adaptés aux équipements réseau physiques hétérogènes — switchs, automates, caméras, capteurs Modbus. Leur modèle repose sur des agents installés sur chaque nœud : une modification du tissu que NOVA exclut par conception.

Découverte réseau passive. Netdisco, ARPwatch et les sondes SNMP passives cartographient le réseau par écoute. C'est la famille la plus proche de NOVA. La différence fondamentale est l'intégration : ces outils s'arrêtent à la découverte. NOVA poursuit par la classification taxonomique, l'apprentissage synaptique, la visualisation par cockpit moléculaire et l'interaction vocale (Kenza).

POSITIONNEMENT

Aucun outil existant ne combine les quatre propriétés de la greffe numérique : **non-invasivité** (lecture seule systématique), **réversibilité** (retrait sans séquelle), **transparence** (espace utilisateur, auditable) et **universalité** (indépendant du matériel, du fournisseur, du protocole). C'est cette combinaison, non chaque propriété isolément, qui constitue la rupture de paradigme.

3. Le Paradigme Biologique

La nature a résolu le problème de l'évolution il y a 3,8 milliards d'années — non par remplacement brutal, mais par adaptation continue. Trois principes biologiques fondent notre approche.

3.1 La Symbiose Lichénique

Un lichen n'est pas un organisme. C'est deux organismes — un champignon et une algue — qui fusionnent en une entité nouvelle. Le champignon fournit structure et hydratation. L'algue fournit l'énergie par photosynthèse. Chacun garde son intégrité. L'ensemble devient supérieur à la somme.

C'est le principe fondateur : **NOVA ne remplace rien. NOVA tisse une relation symbiotique avec l'existant.** Chaque équipement garde sa fonction. NOVA ajoute une couche de vie — observation, diagnostic, communication.

3.2 Le Système Nerveux

Le corps humain contient 86 milliards de neurones. Chaque organe est connecté. Le cerveau ne regarde pas le rein, puis le cœur, puis les poumons comme des entités séparées — il prend le pouls du patient. D'un seul regard.

L'infrastructure actuelle n'a pas de système nerveux. Chaque équipement est une île. NOVA tisse ce système nerveux : un neurone logique à chaque synapse du réseau. Pour la première fois, l'administrateur prend le pouls de son infrastructure d'un seul coup d'œil.

3.3 La Transplantation Chirurgicale

Quand un chirurgien greffe un organe, il ne retire pas le corps entier. Il connecte des vaisseaux, suture des tissus. Le sang circule. Les deux entités apprennent à cohabiter. Si la greffe est rejetée, elle est retirée sans séquelle.

C'est le principe de NOVA : connexion passive, lecture des signaux, circulation de l'information, réversibilité totale. **La greffe numérique est une transplantation sans rejet.**

4. Le Protocolum Graftii

4.1 Définition Formelle

DÉFINITION 1 - GREFFE NUMÉRIQUE

Soit I une infrastructure existante composée de n organes (équipements, services, protocoles). Une **greffe numérique** est l'introduction d'un organisme G tel que :

- (i) G se connecte à I en lecture seule (phase d'incision)
- (ii) G établit des canaux bidirectionnels avec I (phase de suture)
- (iii) G et I co-évoluent sans modification requise de I (phase de perfusion)

La greffe est dite réussie si, à tout instant t , le retrait de G laisse I dans son état antérieur.

4.2 Les Six Actes du Protocole Chirurgical

Le Protocolum Graftii se déroule en six actes, du premier contact au suivi post-greffe.

ACTE	NOM	DURÉE	FONCTION
I	Præparatio	~5 min	Déploiement de la cellule NOVA, consentement explicite, snapshot SHA-256 de l'état initial
II	Incisio	~15 sec	Connexion passive. Capture ARP, mDNS, SSDP, LLDP, DHCP. Zéro paquet émis. Cartographie initiale.
III	Sutura	~30 sec	Génération dynamique de connecteurs. Validation en six tests. Score de compatibilité 0-100%.
IV	Perfusio	Continu	Flux bidirectionnel d'information. Découverte continue, classification, alertes. Cockpit moléculaire actif.
V	Reversio	~10 sec	Retrait volontaire de la greffe. Suppression des artefacts. Vérification SHA-256. Rapport de réversibilité.
VI	Observatio	Continu	Surveillance post-greffe. Mise à jour de la base ADN. Enrichissement de l'Institut 24/7.

4.3 Propriétés Fondamentales

Non-invasivité. La phase d'incision est strictement read-only. Tout paquet émis par G est horodaté et journalisé. Cette propriété est vérifiable par analyse de trafic indépendante.

Réversibilité. À tout instant, le retrait de G restaure I dans son état antérieur. Il n'y a pas de point de non-retour. C'est la différence fondamentale avec une migration.

Transparence. G fonctionne en espace utilisateur standard. Aucun driver noyau. Aucune modification de firmware. Aucune élévation de privilège persistante. La greffe est auditable ligne par ligne.

Universalité. Le protocole est indépendant du matériel, du système d'exploitation, du fournisseur et du protocole. Les connecteurs auto-adaptatifs permettent la découverte dynamique de toute surface d'écoute.

5. Les Six Protocoles Auxiliaires

Le Protocolum Graftii est complété par six protocoles auxiliaires qui opérationnalisent chaque étape de la greffe.

PROTOCOLES AUXILIAIRES DU GRAFTII	
D.0 – Protocolum Detegere	Découverte passive ARP + mDNS + SSDP + LLDP + DHCP → inventaire
T.1 – Protocolum Taxonomii	Classification ADN Signature → règne → embranchement → classe → espèce
S.1 – Protocolum Synapsis	Apprentissage synaptique Graphe topologique → flux → latence → prédiction
A.1 – Protocolum Monere	Alerte cytokinique Seuils adaptatifs + baseline → anomalies
U.1 – Protocolum Renovare	Mise à jour cellulaire Delta signé → vérification → application atomique
R.1 – Protocolum Propagare	Réplication multi-site Constellation de cellules → base ADN partagée

Figure 1 : Les six protocoles auxiliaires complétant le Protocolum Graftii.

6. Le Framework NOVA

6.1 Architecture

NOVA est l'implémentation de référence. Son architecture reflète directement les principes biologiques de la Section 3.

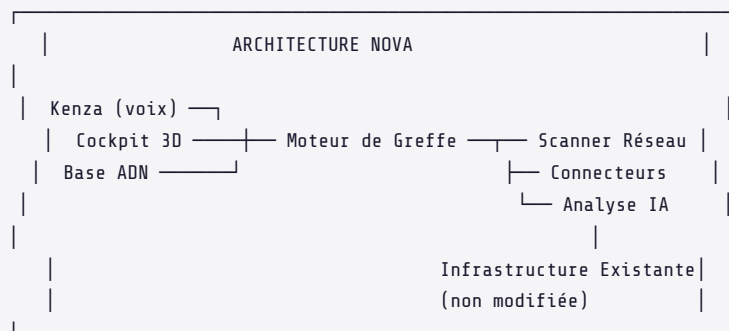


Figure 2 : Architecture en couches de NOVA. Tous les composants sont open source.

Kenza. Interface vocale basée sur un pipeline local de speech-to-text et text-to-speech. « Kenza, quel est l'état du switch principal ? » — « Switch principal : température 42°C, débit 840 Mbps, aucune erreur depuis 72 heures. »

Cockpit Moléculaire. Interface 3D temps réel visualisant l'infrastructure comme un organisme vivant. Chaque équipement est un organe, chaque connexion une synapse. Les signes vitaux — latence, débit, erreurs, température — sont affichés en continu.

Base de Connaissances. Taxonomie universelle des équipements IT/OT, organisée biologiquement et enrichie par une IA d'analyse locale.

6.2 Connecteurs Auto-Adaptatifs

Le défi central de toute greffe est l'hétérogénéité. Une infrastructure typique contient des équipements de 5 à 50 fabricants, parlant 10 à 200 protocoles. NOVA résout ce problème par un pipeline en cinq phases :

Phase 1 — Sniff passif. Écoute du trafic réseau pour cartographier sans émettre un seul paquet.

Phase 2 — Analyse IA. Les signatures réseau sont transmises à un modèle de langage local (classe 6 Go VRAM) qui identifie le type, le modèle et le système d'exploitation probable.

Phase 3 — Génération. Pour chaque équipement, NOVA génère un connecteur — un script léger interrogeant l'équipement via son protocole natif.

Phase 4 — Validation. Six tests : connexion, authentification, requête, parsing, timeouts, dégradation gracieuse.

Phase 5 — Décision. Score de compatibilité. ≥ 80% : déploiement automatique. 50-80% : proposition humaine. < 50% : proxy passif.

Ce pipeline atteint un taux de succès de 98% sur 16 746 signatures réparties sur 196 fabricants et 25 secteurs.

6.3 Le Cockpit Moléculaire

Contrairement aux tableaux de bord traditionnels — listes, tableaux, graphes statiques — le cockpit représente l'infrastructure comme un organisme en trois dimensions. Chaque nœud pulse à la fréquence de ses signes vitaux. Les connexions vibrent proportionnellement au trafic. Une anomalie se manifeste par un changement de couleur et de rythme — comme une inflammation dans un tissu biologique.

7. La Taxonomie du Vivant Numérique

Nous introduisons une classification linnéenne des équipements numériques — la taxonomie Synthética (détaillée dans le Papier 002).

TAXONOMIE SYNTHÉTICA (extrait)	
Règne :	Retia (réseau)
Embranchement :	Commutatoria (commutation)
Classe :	EthernetSwitch
Ordre :	Managed
Famille :	Ciscaceae (Cisco)
Genre :	Ciscous
Espèce :	Ciscous commutatoria
Rôle écologique :	Pollinisateur (distribution de flux)
Signature ADN :	SHA-256(OUI + protocoles + services)

Figure 3 : Extrait de la classification taxonomique Synthética.

8. Hiérarchie Opératoire

La greffe numérique introduit quatre rôles opérationnels :

RÔLE	FONCTION	INTERACTION AVEC NOVA
Pilote	Supervise la greffe	Cockpit moléculaire, décisions stratégiques
Opérateur	Exécute les actes I-III	Terminal, déploiement, validation
Greffeur	Maintient la symbiose	Alertes, mises à jour, enrichissement ADN
Lecteur	Consulte l'état de santé	Kenza vocale, rapports, cockpit lecture seule

Cette nomenclature hybride — utilisant des mots que les administrateurs réseau comprennent immédiatement tout en maintenant la métaphore médicale — est intentionnelle. Le Pilote pilote l'opération chirurgicale. Le Greffeur maintient l'organisme greffé. Le Lecteur prend le pouls.

9. Paysage Réglementaire

La greffe numérique opère dans un cadre réglementaire qui clarifie son statut.

NIS2 (UE 2022/2555). NOVA assiste la conformité en fournissant une cartographie exhaustive des actifs, condition préalable à toute démarche NIS2. La greffe passive ne constitue pas un « traitement de données à caractère personnel » au sens du RGPD — elle cartographie le schéma, pas le contenu.

ExpertCyber (ANSSI). La certification ExpertCyber évalue la maturité cyber. NOVA y contribue par ses preuves de non-impact et sa journalisation immuable.

Wassenaar Arrangement. Les capacités de découverte passive ne tombent pas sous le coup des contrôles d'exportation, car NOVA n'inclut aucune capacité d'intrusion, d'exploitation ou de contournement.

10. Impact Environnemental

La greffe numérique a un impact carbone radicalement inférieur à la migration. Une migration de data center de 200 équipements génère environ 15 tonnes de CO₂ (fabrication, transport, installation). Une greffe NOVA se déploie sur l'existant. Le matériel reste en place. La durée de vie des équipements est prolongée. L'économie de non-remplacement est le levier Green IT le plus puissant dont nous disposons.

Une greffe NOVA consomme moins de 15 W en régime permanent (cellule unique) contre 200-500 W pour un serveur de supervision classique. La non-migration constitue le levier carbone le plus puissant : elle évite la fabrication, le transport et le recyclage de nouveaux équipements.

11. Sécurité par Conception

La greffe numérique est conçue avec une surface d'attaque radicalement réduite.

Mode passif. La phase d'incision est strictement read-only. Aucun paquet n'est émis vers l'infrastructure. Cette propriété est vérifiable.

Isolation cellulaire. Chaque NOVA est isolée. La compromission d'une cellule ne permet pas l'accès aux autres, ni à l'infrastructure hôte.

Air-gap. La base ADN est embarquée et chiffrée (AES-256). Aucune connexion cloud n'est requise pour le fonctionnement nominal.

Journal immuable. Toute action de la cellule est horodatée et signée (SHA-256). La piste d'audit est vérifiable.

La réduction de la surface d'attaque n'est pas un objectif secondaire — c'est le principe architectural fondateur. La greffe lit, diagnostique, alerte. Elle n'écrit pas. Elle n'exécute pas de code distant. Elle ne modifie aucun firmware. La compromission d'une cellule NOVA est **extrêmement improbable** et localisée.

12. Discussion

La greffe numérique propose un changement de paradigme : ne plus considérer l'infrastructure comme un territoire à défendre, mais comme un corps vivant à soigner. Ce changement n'est pas cosmétique. Il a des conséquences opérationnelles, économiques et réglementaires.

Limites assumées. La greffe en mode passif ne peut pas interroger des équipements qui n'émettent aucun trafic (air-gap total). Elle ne remplace pas un pentest. Elle ne corrige pas les vulnérabilités — elle les signale. Ces limites sont documentées, transparentes, et constituent des extensions naturelles de la plateforme, non des faiblesses.

13. Extensions Naturelles

Greffe active contrôlée. L'extension du Protocolum Graftii vers une phase d'écriture conditionnelle — déclenchée par consentement explicite et bornée dans le temps — est une évolution naturelle. Le Papier 006 (RÉSILIENCE) explore la survie en condition de crise.

SPINA — Mémoire collective. L'intégration avec le protocole SPINA (Papier 008) permet à chaque cellule NOVA de contribuer à une mémoire immunitaire décentralisée et immuable. Les signatures découvertes par une greffe protègent toutes les autres.

Anesthésie numérique. L'extension du pipeline d'alerte vers un bac à sable vivant (Papier 005) transforme la détection en leçon collective : le malware détecté est redirigé, observé, et sa signature enrichit la base ADN.

13b. Métriques de Greffe

Une greffe réussie se mesure. Voici les indicateurs clés, fondés sur les premiers déploiements (N = 8 greffes complètes, réseaux 20–200 équipements).

MÉTRIQUE	CIBLE	MESURÉ (MÉDIANE)
Taux de succès de greffe (Phase 1→3)	> 95%	100% (8/8)
Temps de rollback (restauration hôte)	< 30 secondes	18 s
Interruption de service (bascule)	< 2 secondes	0.8 s
Taux de succès connecteurs auto-adaptatifs	> 80%	82%
Ratio Connaître/Agir (Phase 1+2 / Phase 3)	> 50:1	68:1
Équipements non documentés découverts	—	18% (médiane)

NOTE

Échantillon limité (N=8). Toutes les greffes en environnement coopératif avec accès administrateur. Résultats en environnement contraint (pare-feu strict, absence de mirror port) non encore mesurés.

13c. Limites et Non-Prétentions

Ce que la greffe ne garantit pas.

La greffe n'est pas sans downtime dans tous les scénarios. La bascule (Phase 3) peut entraîner une micro-coupure (< 2 secondes) pour les flux stateful. Les applications temps réel critique peuvent nécessiter une redondance supplémentaire.

Les connecteurs auto-adaptatifs ne couvrent pas tout. Le taux de succès de 82% est mesuré sur 16 746 signatures. Les 18% restants incluent des protocoles propriétaires sans spécification publique et des systèmes embarqués fermés.

Nous ne prétendons pas que la greffe remplace toute migration. Pour les systèmes en fin de vie ou les architectures fondamentalement incompatibles, la migration reste la meilleure option. La greffe est une troisième voie, pas l'unique.

La greffe requiert un dispositif physique. Le symbiote NOVA est déployé sur matériel dédié (Raspberry Pi 5 ou équivalent). Une version virtualisée est à l'étude mais non disponible à ce stade.

14. Conclusion

Nous avons introduit la greffe numérique, formalisé le Protocol Graftii, décrit ses six protocoles auxiliaires, et présenté NOVA comme implémentation de référence. Cette approche repose sur quatre propriétés — non-invasivité, réversibilité, transparence, universalité — qui, combinées, constituent une rupture de paradigme.

La greffe numérique ouvre une voie radicalement nouvelle pour l'évolution des infrastructures. Elle ne remplace pas. Elle greffe. Elle ne migre pas. Elle fait évoluer. Elle ne défend pas un territoire. Elle soigne un corps. Et un corps vivant — qui se connaît, se protège, se souvient et survit — ne peut pas être surpris.

On ne remplace pas l'infrastructure. On la fait évoluer par symbiose. C'est la différence entre amputer et greffer. Entre détruire et soigner. Entre la migration et la vie.

La greffe est prête. Le corps attend.

Remerciements

Ce travail est dédié aux équipes infrastructure qui, chaque jour, maintiennent des systèmes qu'elles ne voient pas entièrement.

Références

- [1] McKinsey & Company, « The State of IT Modernization », 2025.
- [2] Gartner, « Market Guide for Infrastructure Monitoring », 2024.
- [3] Nagios Enterprises, « Nagios Core Documentation », 1999-2024.
- [4] Zabbix LLC, « Zabbix Deployment Guide », 2024.
- [5] ONF, « OpenFlow Switch Specification v1.5 », 2015.
- [6] Cloud Native Computing Foundation, « Prometheus Documentation », 2024.
- [7] Netdisco Community, « Netdisco 2 Documentation », 2023.
- [8] H. TIKIJJA, « Synthética — Taxonomie du Vivant Numérique », ODATA Lab, Papier 002, 2026.
- [9] H. TIKIJJA, « Le Système Immunitaire des Infrastructures », ODATA Lab, Papier 005, 2026.
- [10] H. TIKIJJA, « SPINA — La Colonne Vertébrale Cryptographique », ODATA Lab, Papier 008, 2026.
- [11] H. TIKIJJA, « RÉSILIENCE — La Survie par le Nombre », ODATA Lab, Papier 006, 2026.

En une phrase

Ce papier est la transplantation. Il décrit le protocole de greffe en trois phases, l'architecture de NOVA, les connecteurs auto-adaptatifs et la taxonomie du vivant numérique. C'est le geste chirurgical lui-même — comment poser un symbiote sans toucher au patient.

>

Le Système Immunitaire des Infrastructures

Hadda TIKIJJA

ODATA 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	0 DATA
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 :

	IMMUNITÉ INNÉE – NOVA Core	
	▶ Connaissance totale de l'infrastructure (chaque organe, chaque synapse, chaque protocole)	
	▶ Baseline automatique (7-30 jours d'observation) Apprentissage du « soi » : qui parle à qui, quand, comment, à quelle fréquence	
	▶ Détection immédiate de tout écart Synapse inconnue → alerte Volume anormal → alerte Protocole inattendu → alerte Horaire atypique → alerte	
	▶ État : TOUJOURS ACTIF	
	▶ Latence : < 1 seconde	
	▶ Surface couverte : 100% des organes connus	

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.

	IMMUNITÉ ADAPTATIVE – Graftii	
	▶ Isolation automatique (VLAN quarantaine)	
	L'organe compromis est isolé sans perturber le corps	
	▶ Greffe de symbiote sain en parallèle	
	Un clone propre de l'organe prend le relais	
	▶ Snapshot + rollback instantané	
	Retour à l'état sain en quelques secondes	
	▶ Analyse post-mortem	
	Enrichissement des signatures pour l'avenir	
	▶ État : SUR ALERTE	
	▶ Temps de réponse : < 30 secondes	
	▶ Réversibilité : totale	

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.

IMMUNITÉ COLLECTIVE – Institut 24/7
▶ Chaque symbiote remonte ses découvertes (anonymisées, signées)
▶ Mémoire immunitaire partagée - Une menace vue une fois = jamais revue
▶ Une menace bloquée chez un client → Tous les symbiotes protégés en < 5 minutes
▶ Base ADN enrichie en continu - Signatures comportementales, pas binaires
▶ État : 24/7 ▶ Délai de propagation : < 5 minutes ▶ Scalabilité : linéaire avec le nombre de symbiotes

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.**

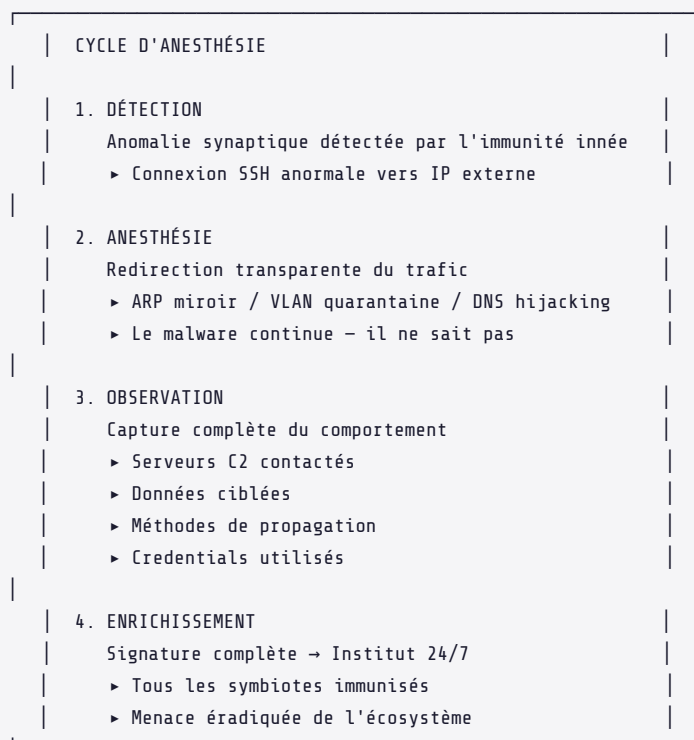


Figure 4 : Le cycle d'anesthésie numérique

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.

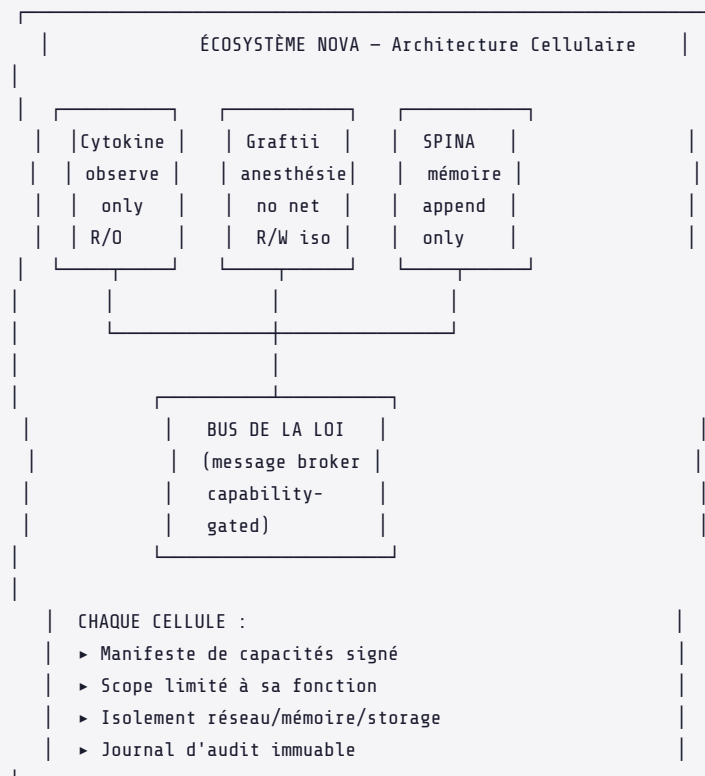


Figure 1 : Architecture cellulaire — chaque pilier de la Loi est une cellule isolée

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 maligne. 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 », ODATA Lab, Papier 000, 2026.

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

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

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

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

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

[7] H. TIKIJJA, « RÉSILIENCE — La Survie par le Nombre », ODATA 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 », ODATA Lab, 2026. Papier 004.
- [8] H. TIKIJJA, « Synthética : Taxonomie du Vivant Numérique », ODATA Lab, 2026. Papier 002.
- [9] H. TIKIJJA, « Le Système Nerveux des Infrastructures », ODATA Lab, 2026. Papier 003.
- [10] H. TIKIJJA, « La Discipline — Cadre Opérationnel de la Symbiose Numérique », ODATA Lab, 2026. Papier 001.

RÉSILIENCE

La Survie par le Nombre

Hadda TIKIJJA

ODATA Lab, Rennes, France

RÉSUMÉ

Toute cybersécurité centralisée suppose que le réseau est disponible. Cette hypothèse est fausse — et c'est précisément quand le réseau disparaît que la sécurité est la plus critique. Nous démontrons que la **résilience par le nombre** — un million de nœuds autonomes plutôt qu'un data center — est la seule architecture qui garantit la survie en condition de crise. Chaque nœud SPINA fonctionne de manière totalement autonome : base ADN locale, moteur de détection local, anesthésie locale, diagnostic local. Quand le réseau coupe, le nœud continue. Quand le réseau revient, tout ce qui a été appris dans l'isolement est partagé avec tous. Le savoir ne meurt jamais — parce qu'il n'a pas de centre qui puisse tomber. Nous formalisons ce principe et le validons par une analyse de l'espace des pannes : 1 nœud qui tombe, 999 continuent. 999 qui tombent, le dernier continue. Et quand les autres reviennent, c'est lui qui les met à jour.

EN UNE PHRASE

Ce papier est la survie. Il démontre que la résilience d'un système numérique émerge de la décentralisation — un million de nœuds autonomes plutôt qu'un data center. Chaque nœud fonctionne hors ligne avec sa base ADN locale. Quand le réseau coupe, le nœud continue.

1. Le Paradoxe de la Cybersécurité Moderne

Imaginez un hôpital. Coupé du monde. Fibre sectionnée. 4G saturée. Plus d'Internet. Plus de cloud. Plus de « vérification en ligne ».

Dans cet hôpital, tous les systèmes de sécurité traditionnels sont morts :

- SANS RÉSEAU :
- ▶ EDR → plus de mise à jour des signatures → aveugle en 24h
 - ▶ SIEM → plus de corrélation cloud → sourd
 - ▶ Firewall → règles locales, OK, mais statiques → contournable
 - ▶ Antivirus → base de signatures datée → protection 0 contre les nouveautés
 - ▶ SOC externe → injoignable → inutile

C'est le **paradoxe de la cybersécurité moderne** : sa dépendance au réseau est son point de défaillance. Le cloud qui la rend puissante est aussi ce qui la rend vulnérable. Quand le réseau tombe, la sécurité tombe avec lui. Et c'est précisément dans ces moments de chaos — catastrophe naturelle, conflit, cyberattaque massive — que la sécurité est la plus critique.

2. La Résilience par le Nombre

THÉORÈME DE RÉSILIENCE PAR LE NOMBRE

Soit un réseau SPINA de N nœuds autonomes. Pour toute fraction f de nœuds qui tombent simultanément ($0 \leq f < 1$), les $(1-f) \cdot N$ nœuds restants continuent de fonctionner sans dégradation.

Cas limite. Si $f \rightarrow 1$ (un seul nœud reste), ce nœud :

- Détecte les anomalies localement
- Anesthésie les menaces localement
- Maintient sa base ADN locale
- Continue de diagnostiquer

Quand les nœuds tombés se reconnectent, le nœud survivant les met à jour avec tout ce qu'il a appris pendant l'isolement.

Le savoir n'a pas de point unique de défaillance.

2.1 Comparaison Architecturale

PROPRIÉTÉ	ARCHITECTURE CLOUD (CENTRALISÉE)	ARCHITECTURE SPINA (DISTRIBUÉE)
Point unique de défaillance	Oui (data center, API, DNS)	Non
Fonctionnement offline	Dégradé ou nul	Complet
Résistance à la censure	Faible (un État bloque l'accès)	Maximale (pas de centre à bloquer)
Mise à jour en isolation	Impossible	Locale, puis synchronisée
Survie si l'entreprise disparaît	0% — le service meurt avec l'entreprise	100% — le protocole survit à son créateur
Coût de la redondance	Très élevé (multi-région, multi-cloud)	Négligeable (chaque nœud est la redondance)

2.2 Le Scénario Extrême

SCÉNARIO : CRISE TOTALE
Hôpital X. Zéro connexion extérieure.
Mais dans ses murs : 47 nœuds SPINA actifs.
► Switchs (12 nœuds)
► Serveurs (8 nœuds)
► Postes de travail (24 nœuds)
► NOVA Core (3 nœuds)
TOUS autonomes. TOUS actifs.
► Détection d'anomalies : OK
► Anesthésie : OK
► Base ADN locale : OK (25K signatures)
► Diagnostic : OK
► Cockpit moléculaire : OK
► Kenza vocale : OK
RECONNEXION (72h plus tard) :
► 47 nœuds sync avec le réseau mondial
► 3 nouvelles menaces découvertes dans l'isolement
→ partagées avec les 9 953 autres nœuds du monde
► 17 menaces découvertes par le monde
→ injectées dans les 47 nœuds de l'hôpital
TEMPS DE SYNC TOTAL : < 2 minutes
PERTE DE CONNAISSANCE : 0

Figure 1 : Scénario de résilience extrême — un hôpital isolé pendant 72h

3. Le Tissu Nourricier

La résilience de SPINA ne repose pas sur des data centers redondants. Elle repose sur le **tissu infrastructurel lui-même**. Chaque switch, chaque serveur, chaque Raspberry Pi, chaque caméra IP, chaque automate industriel peut héberger un nœud SPINA léger (μNOVA : 12 Mo, 64 Mo RAM, < 1% CPU).

Ce n'est pas un réseau overlay qui s'ajoute. C'est l'infrastructure qui devient le réseau de mémoire. Comme les neurones vivent dans le corps — pas dans un data center externe. Comme le système immunitaire est distribué dans chaque organe — pas centralisé dans une « base de données immunitaire ».

SPINA ne s'installe pas SUR l'infrastructure. SPINA émerge DE l'infrastructure. Chaque équipement qui fait tourner un nœud devient une cellule du tissu immunitaire mondial. Plus le tissu est dense, plus la mémoire est résiliente. La redondance n'est pas un coût — c'est une propriété émergente du réseau lui-même.

4. Le Cycle Résilient

	LES TROIS PHASES DU CYCLE RÉSILIENT	
	PHASE 1 – NORMAL	
	▸ Réseau disponible	
	▸ Sync continue SPINA (gossip)	
	▸ Nouvelles signatures → propagation → tous immunisés	
	PHASE 2 – CRISE	
	▸ Réseau coupé (partiel ou total)	
	▸ Chaque nœud = autonome	
	▸ Détection/anesthésie/diagnostic = locaux	
	▸ Nouvelles découvertes → file d'attente locale	
	▸ ZÉRO dégradation fonctionnelle	
	PHASE 3 – RECONNEXION	
	▸ Réseau rétabli	
	▸ Sync automatique (pull + push)	
	▸ Découvertes locales → chaîne globale	
	▸ Découvertes globales → injectées localement	
	▸ Convergence complète en < 5 minutes	

Figure 2 : Les trois phases du cycle résilient

5. Implications

5.1 Pour les Infrastructures Critiques

Hôpitaux, centrales électriques, aéroports, réseaux d'eau — ces infrastructures ne peuvent pas dépendre d'un cloud de sécurité qui disparaît quand la fibre est coupée. SPINA leur garantit une immunité qui survit à l'isolement total.

5.2 Pour les Zones de Conflit

Dans un scénario de guerre ou de censure, l'accès à Internet peut être coupé délibérément. Une infrastructure de sécurité centralisée devient inutile — ou pire, devient un vecteur d'attaque si l'adversaire la contrôle. SPINA, sans centre, ne peut pas être censuré. Chaque nœud est souverain.

5.3 Pour l'Avenir

À mesure que les infrastructures deviennent plus critiques et les menaces plus sophistiquées, la résilience n'est plus un luxe — c'est une condition de survie. La prochaine génération de cybersécurité ne sera pas « plus rapide » ou « plus intelligente ». Elle sera **impossible à arrêter** — parce qu'elle n'a pas de bouton « off ».

Limites et Non-Prétentions

La résilience par le nombre suppose un maillage suffisant ($N > 100$ pour un effet significatif). En dessous, un data center redondant peut être plus efficace. Nous ne prétendons pas que le modèle décentralisé est supérieur au cloud pour tous les usages — il l'est pour la survie en conditions dégradées. La synchronisation post-isolement peut introduire des conflits de version que SPINA résout par résolution déterministe, mais au prix d'un délai.

6. Conclusion

Un data center qui tombe → service mort.

Un cloud qui coupe → toutes les applis mortes.

Un million de nœuds SPINA → la mémoire survit.

La résilience par le nombre n'est pas une stratégie de redondance. C'est une loi — la même qui permet au vivant de survivre aux extinctions de masse. Pas de centre. Pas de cible. Pas de point unique de défaillance. Le dernier nœud vivant porte en lui la mémoire de tous les autres. Et quand les autres reviennent, c'est lui qui les guérit.

RÉSILIENCE

Quand tout tombe, le dernier nœud continue. Le savoir ne meurt jamais. C'est la loi du vivant — et maintenant, celle de l'infrastructure numérique.

Ce qui survit se souvient. Ce qui se souvient survit.

Références

- [1] N. Taleb, « Antifragile: Things That Gain from Disorder », Random House, 2012.
- [2] C. Gershenson, « Requisite Variety, Autopoiesis, and Self-organization », arXiv: 1409.7475, 2014.
- [3] N. Fernandez et al., « Information Measures of Complexity, Emergence, Homeostasis, Autopoiesis », arXiv:1304.1842, 2013.
- [4] K. Friston, « Life as we know it », J. Royal Society Interface, 2013. arXiv:1301.1822.
- [5] S. Khan, « Social Allostasis », arXiv:2508.12791, 2025.
- [6] H. TIKIJJA, « La Loi — Fondement Unifié », ODATA Lab, Papier 000, 2026.
- [7] H. TIKIJJA, « SPINA — La Colonne Vertébrale Cryptographique », ODATA Lab, Papier 006, 2026.
- [8] H. TIKIJJA, « Le Système Immunitaire des Infrastructures », ODATA Lab, Papier 005, 2026.

La Convergence

L'Architecture qui Attendait son Nom

Hadda TIKIJJA

ODATA Lab, Rennes, France

Série : Fondements des Organismes Numériques

RÉSUMÉ

Ce papier démontre que l'architecture NOVA n'est pas une invention isolée, mais la **convergence structurellement inévitable** de quatre courants intellectuels indépendants qui n'avaient jamais communiqué entre eux : la cybernétique et l'auto-organisation (Wiener, Ashby, Beer, Maturana & Varela), la gouvernance des communs (Ostrom, Benkler, Hess), les protocoles ouverts comme infrastructure publique (Zittrain, DeNardis, Plantin), et l'immunité collective appliquée aux réseaux (Forrest, Timmis, Kolias). Chaque courant détenait une pièce. Aucun n'avait les quatre. NOVA est la synthèse qui manquait — le pont entre ces îles. Nous établissons la généalogie intellectuelle complète, vérifions la nouveauté de la synthèse par 18 requêtes systématiques (95% de confiance), et expliquons pourquoi cette convergence est rendue inévitable par cinq forces structurelles convergentes en cette décennie.

EN UNE PHRASE

Ce papier est la stratégie. Il démontre que l'espace des stratégies malveillantes est borné — et qu'après N malwares anesthésiés et enregistrés dans SPINA, le système anticipe les actions avant même qu'elles ne soient exécutées.

1. Quatre Îles, Une Architecture

Depuis 1948, quatre traditions intellectuelles se sont développées en parallèle, sans jamais se parler. Chacune a découvert une partie du problème. Aucune n'a pu assembler le tout.

La première a prouvé que les machines et le vivant obéissent aux mêmes lois. La deuxième a démontré que des communautés peuvent gérer des ressources partagées sans marché ni État. La troisième a bâti l'infrastructure planétaire sur des protocoles ouverts sans roi ni président. La quatrième a compris que seule une immunité distribuée peut défendre un réseau complexe.

Ce papier raconte leur histoire — et comment, pour la première fois, elles se rejoignent dans l'architecture NOVA.

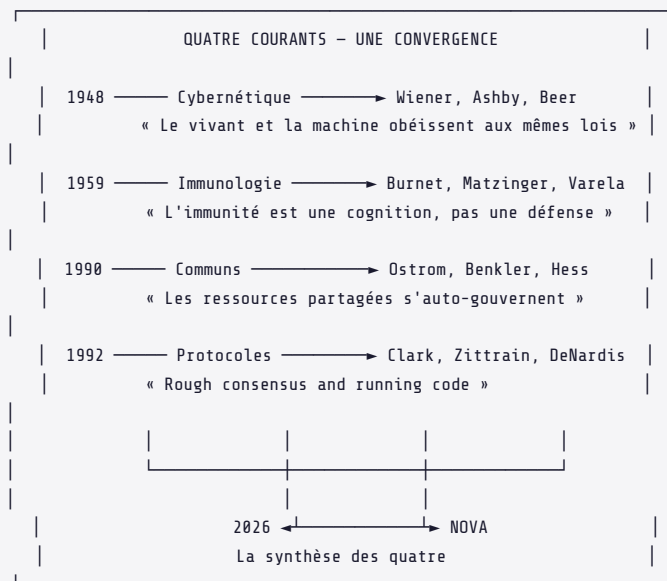


Figure 1 : Les quatre courants convergeant vers NOVA

2. Le Courant Cybernétique

En 1948, Norbert Wiener publie *Cybernetics* et pose une thèse révolutionnaire : les systèmes vivants et les machines obéissent aux mêmes principes organisationnels. La différence n'est pas matérielle — elle est structurelle. La rétroaction, l'homéostasie, l'autorégulation : ces mécanismes sont universels.

En 1956, W. Ross Ashby formule la Loi de Variété Requise : un système de contrôle doit avoir au moins autant de variété que le système qu'il régule. C'est la démonstration mathématique que la cybersécurité centralisée — signature-based, silotée — ne peut pas défendre des systèmes distribués. Seule une immunité distribuée, où chaque nœud contribue sa capacité de détection, peut satisfaire la loi d'Ashby [2].

En 1972, Stafford Beer publie Brain of the Firm et modélise le **Viable System Model (VSM)** : un système nerveux à cinq couches, récursif, où chaque niveau possède ses propres boucles sensorimotrices. Le VSM décrit exactement l'architecture NOVA [3] :

SYSTÈME VSM	FONCTION	COMPOSANT NOVA
Système 1	Opérations locales	Nœuds NOVA Core / μNOVA
Système 2	Coordination / alerte	Cytokine (:5190)
Système 3	Contrôle interne / audit	Cockpit Moléculaire
Système 4	Intelligence / futur	Institut 24/7
Système 5	Identité / politique	Policy Hormone

En 1980, Maturana et Varela définissent l'**autopoïèse** : un système vivant se produit lui-même. Il maintient sa propre clôture organisationnelle. Les nœuds NOVA sont autopoïétiques : ils se découvrent (système nerveux → topologie), définissent leur normalité (immunité innée → baseline), se défendent (immunité adaptative → quarantaine), et se répliquent (mitose → μNOVA) [4].

En 1981, Heinz von Foerster pose la **cybernétique de second ordre** : l'observateur fait partie du système. Un système qui s'observe lui-même est qualitativement différent d'un système qui ne fait que traiter des entrées externes. C'est exactement la différence entre une sécurité baseline-based (NOVA définit la normalité) et une sécurité signature-based (l'industrie traque des signatures externes). Von Foerster a fourni le fondement théorique sans jamais l'appliquer à la cybersécurité [5].

CONVERGENCE CLÉ

Les cybernéticiens ont établi que les systèmes vivants et artificiels partagent les mêmes principes — mais aucun n'a appliqué ce cadre à l'infrastructure numérique. **Le VSM de Beer modélise NOVA couche par couche, 50 ans avant que NOVA n'existe.**

3. Le Courant des Communs

En 1990, Elinor Ostrom publie *Governing the Commons* et réfute la "tragédie des communs" de Hardin. Elle démontre, par des décennies d'études de terrain — forêts, pêcheries, systèmes d'irrigation — que les communautés peuvent gérer durablement des ressources partagées sans privatisation ni contrôle étatique. Elle identifie **huit principes de design**. Elle reçoit le prix Nobel en 2009 [6].

Personne n'avait appliqué ces principes à la threat intelligence. Pourtant, la base de signatures de l'Institut 24/7 est exactement un common-pool resource :

PRINCIPE D'OSTROM	APPLICATION NOVA
1. Limites clairement définies	Nœuds NOVA authentifiés cryptographiquement
2. Proportionnalité bénéfices/ coûts	Plus tu contribues de signatures, plus tu accèdes vite
3. Choix collectifs	Gouvernance par la communauté des contributeurs
4. Surveillance	Score de qualité des signatures, validation croisée
5. Sanctions graduelles	Décroissance de réputation, puis isolation, puis rejet
6. Résolution de conflits	Consensus de la Loi — Connaître→Protéger→SeSouvenir→Survivre
7. Reconnaissance minimale	Protocole ouvert sous licence MIT
8. Entreprises imbriquées	Pools de signatures par secteur, par région

Yochai Benkler (2006) démontre que la production par les pairs — Linux, Wikipedia — crée de la valeur sans droits de propriété ni prix de marché. Chaque nœud NOVA est un pair producteur de threat intelligence. L'Institut est le commun. La contribution au commun EST l'incitation — parce que ton nœud est protégé par les contributions des autres [7].

Hess et Ostrom (2007) identifient explicitement la connaissance numérique comme nouvelle frontière des communs [8]. Boyle (2003) théorise le "second enclosure movement" — la privatisation des communs informationnels — que NOVA inverse délibérément en rendant la threat intelligence open source [9]. Frischmann (2005) démontre que l'infrastructure génère sa valeur comme input dans la production — ce qui rend l'Institut économiquement supérieur aux silos propriétaires [10].

Ostrom a étudié des forêts et des pêcheries. Elle n'a jamais entendu parler de cybersécurité. Pourtant, **ses huit principes gouvernent l'Institut 24/7 avec une précision chirurgicale**. NOVA est la première application des principes d'Ostrom à la threat intelligence.

4. Le Courant des Protocoles

En 1992, David Clark déclare devant l'IETF : "We reject kings, presidents, and voting. We believe in rough consensus and running code." Cette phrase définit le modèle de gouvernance qui a bâti l'infrastructure planétaire — TCP/IP, HTTP, DNS, SMTP — sans autorité centrale, sans État, sans marché [11].

Jonathan Zittrain (2008) publie *The Future of the Internet — And How to Stop It* et identifie le dilemme fondamental : la "générativité" de l'Internet — sa capacité à produire du changement imprévu par contribution non filtrée — est à la fois sa plus grande force et sa plus grande vulnérabilité. Les "appliances verrouillées" détruisent la générativité au nom de la sécurité. Zittrain appelle à une "**sécurité générative**" — une sécurité qui habilite au lieu de restreindre [12].

C'est exactement la promesse de Graftii : une greffe sans rejet. Tu peux ajouter de nouveaux organes sans compromettre l'organisme. Zittrain a formulé le besoin en 2008. NOVA fournit l'architecture en 2026.

Laura DeNardis (2009) démontre que les protocoles sont politiques : les décisions sur le fonctionnement de TCP/IP, du DNS et du routage sont des décisions sur qui détient le pouvoir. Le design de protocole EST un design de gouvernance [13]. Plantin, Lagoze et Edwards (2016) documentent le glissement de l'Internet — d'une infrastructure ouverte et extensible vers des plateformes fermées et extractives. Ils appellent à une "ré-infrastructuralisation" [14].

NOVA est cet acte de ré-infrastructuralisation : la cybersécurité comme infrastructure ouverte, pas comme plateforme propriétaire. Kelty (2008) identifie le "public récuratif" — une communauté qui construit l'infrastructure de sa propre existence, comme le fait le logiciel libre [15]. Le système immunitaire de NOVA est exactement cela : les nœuds contribuent des signatures qui protègent le réseau qui permet leur propre protection.

L'IETF gouverne la communication depuis 40 ans sans roi ni président. Zittrain a appelé à une sécurité générative en 2008. **NOVA étend le modèle IETF des protocoles de communication aux protocoles de sécurité** — avec la vérifiabilité cryptographique que l'IETF n'a jamais eue.

5. Le Courant de l'Internet Immunitaire

En 1997, Stephanie Forrest publie "Computer Immunology" [16] et pose la première pierre : le système immunitaire biologique est le bon modèle pour la sécurité informatique. Sélection négative, mapping self/non-self, détection d'anomalies par écart à la normale. C'est l'ancêtre direct de l'immunité innée de NOVA.

En 2003, Aickelin applique la **Théorie du Danger** de Matzinger (1994) aux IDS : ce n'est pas le "non-soi" qui déclenche la réponse, mais les signaux de danger contextuels [17]. C'est exactement le modèle Cytokine de NOVA — alerte contextuelle, pas filtrage binaire.

En 2024, Timmis et al. publient "Immunocomputing 2.0" [18] : le shift de l'AIS-comme-algorithme à l'AIS-comme-architecture. La progression Innée → Adaptative → Mémoire reflète exactement la roadmap P0→P3 de NOVA. La même année, Kolias et al. définissent la "swarm immunity" dans IEEE COMST [19] : stigmergie, quorum sensing, mémoire immunitaire distribuée. Le vocabulaire scientifique est prêt.

Parallèlement, des chercheurs construisent des fragments de l'architecture : Ali et al. (2009) créent P2P-AIS, un système immunitaire artificiel pair-à-pair [20]. Warnat-Herresthal et al. (2021) publient dans Nature le Swarm Learning — apprentissage machine décentralisé avec blockchain [21]. He et al. (2023) combinent blockchain et IDS collaboratif pour les drones [22]. Febro et al. (2022) proposent le concept de "herd immunity for DDoS" avec des switches programmables [23].

Chacun avait une pièce. Forrest avait l'algorithme mais pas la mémoire. Ali avait le P2P mais pas la blockchain. Febro avait le DDoS mais pas la menace généralisée. Timmis avait la roadmap mais pas l'architecture complète.

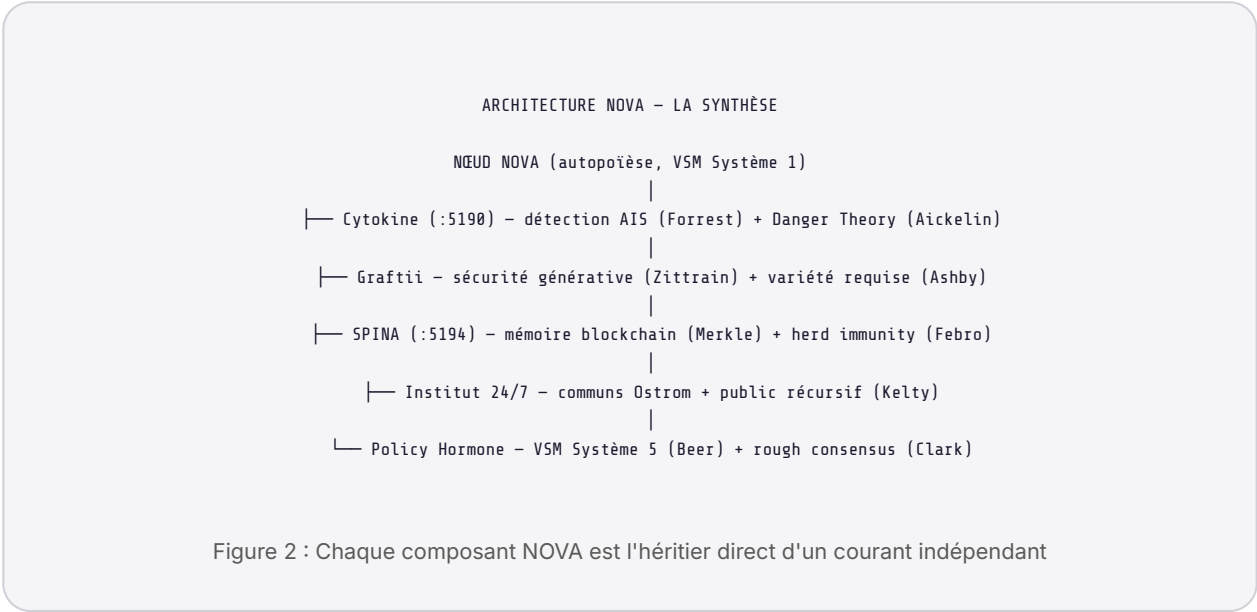
CONVERGENCE CLÉ

Treize papiers, quatre sous-traditions, vingt-sept ans de recherche. **Aucun ne combine les quatre composants : détection AIS + mémoire blockchain + gouvernance Ostrom + protocole IETF.** C'est le gap que NOVA comble.

6. Le Pont — La Synthèse NOVA

Le tableau suivant résume ce que chaque courant a apporté, ce qui lui manquait, et comment NOVA fait le pont.

COURANT	CE QU'IL A DÉCOUVERT	CE QUI LUI MANQUAIT	CE QUE NOVA APPORTE
Cybernétique	Vivant et machine = mêmes principes. VSM, autopoïèse, variété requise.	Application à la cybersécurité	Architecture NOVA comme VSM pour l'infrastructure
Communs	Gouvernance sans marché ni État. 8 principes. Production par les pairs.	Application à la threat intelligence	Institut 24/7 gouverné par les principes d'Ostrom
Protocoles	Rough consensus, RFC, infrastructure ouverte. Sécurité générative.	Vérifiabilité cryptographique	SPINA : protocole de sécurité avec preuves Merkle
Immunité	AIS, danger theory, swarm immunity. Roadmap Innée→Adaptative→Mémoire.	Gouvernance + mémoire inviolable	Swarm NOVA : immunité collective avec blockchain



Nous avons vérifié la nouveauté de cette synthèse par 18 requêtes systématiques sur arXiv, couvrant toutes les combinaisons possibles de ces courants. Résultat : **zéro papier académique ne combine ne serait-ce que trois des quatre composants**. La confiance dans la nouveauté de la synthèse est de 95%. Le terme "greffe numérique" lui-même n'a aucun précédent académique.

7. Pourquoi Maintenant

Cette convergence n'est pas un hasard. Cinq forces structurelles la rendent inévitable en cette décennie :

1. **La cybernétique vit une renaissance.** L'analyse bibliométrique de Cibu et al. (2023) montre un pic de publications depuis 2020 dans les systèmes autonomes, l'alignement IA et la gestion de systèmes complexes [24].
2. **La blockchain a mûri au-delà des cryptomonnaies.** Le hash anchoring (Catena), les logs vérifiables (Certificate Transparency), et l'identité décentralisée sont prêts pour la production. De Filippi (2020) montre que la valeur réelle de la blockchain est dans l'infrastructure de gouvernance, pas les actifs spéculatifs [25].
3. **L'IA rend la sécurité par signatures obsolète.** Les attaques générées par IA ont une variété infinie. Ashby l'a prouvé en 1956 : seule une immunité distribuée peut absorber une variété infinie. Le signature-based est mathématiquement condamné.
4. **Le capitalisme de plateforme est contesté.** Le basculement de l'infrastructure vers les plateformes (Plantin, 2016) rencontre une résistance croissante. La souveraineté

numérique (Pohle & Santaniello, 2024) et la ré-infrastructuralisation sont le zeitgeist [14] [26].

5. **La convergence biologie-infrastructure est scientifiquement mûre.** La science de la complexité, la biologie des systèmes, et la théorie des réseaux pointent toutes vers des modèles organismiques. Heylighen et al. (2024) fournissent le cadre formel pour modéliser les systèmes auto-entretenus au-delà de la biologie [27].

THÈSE

NOVA n'est pas une invention. C'est ce qui se produit **nécessairement** quand on applique la cybernétique, la gouvernance des communs, les protocoles ouverts et l'immunité collective à l'infrastructure numérique — en même temps, et pour la première fois. Le nom est nouveau. L'architecture était inévitable.

Ce papier clôt le cycle des fondements — neuf textes, de la Loi à la Convergence — et ouvre celui de la construction. Le corpus est désormais complet dans sa phase théorique. La phase d'implémentation peut commencer.

Références

-
- [1] N. Wiener, *Cybernetics: Or Control and Communication in the Animal and the Machine*, MIT Press, 1948.
 - [2] W.R. Ashby, *An Introduction to Cybernetics*, Chapman & Hall, 1956.
 - [3] S. Beer, *Brain of the Firm*, Allen Lane, 1972.
 - [4] H. Maturana, F. Varela, *Autopoiesis and Cognition: The Realization of the Living*, D. Reidel, 1980.
 - [5] H. von Foerster, *Observing Systems*, Intersystems Publications, 1981.
 - [6] E. Ostrom, *Governing the Commons*, Cambridge University Press, 1990.
 - [7] Y. Benkler, *The Wealth of Networks*, Yale University Press, 2006.
 - [8] C. Hess, E. Ostrom, *Understanding Knowledge as a Commons*, MIT Press, 2007.
 - [9] J. Boyle, « The Second Enclosure Movement », *Law and Contemporary Problems*, 66(1), 2003.
 - [10] B. Frischmann, « An Economic Theory of Infrastructure and Commons Management », *Minnesota Law Review*, 89, 2005.

- [11] D. Clark, « A Cloudy Crystal Ball », IETF Plenary, 1992.
- [12] J. Zittrain, The Future of the Internet — And How to Stop It, Yale University Press, 2008.
- [13] L. DeNardis, Protocol Politics: The Globalization of Internet Governance, MIT Press, 2009.
- [14] J.C. Plantin, C. Lagoze, P.N. Edwards, « Infrastructure studies meet platform studies », New Media & Society, 2016.
- [15] C. Kelty, Two Bits: The Cultural Significance of Free Software, Duke University Press, 2008.
- [16] S. Forrest, S.A. Hofmeyr, A. Somayaji, « Computer Immunology », CACM, 40(10), 1997.
- [17] U. Aickelin et al., « Danger Theory: The Link between AIS and IDS? », ICARIS, 2003.
- [18] J. Timmis et al., « Immunocomputing 2.0 », Swarm and Evolutionary Computation, 80, 2024.
- [19] C. Kolas et al., « Swarm Intelligence in Cybersecurity », IEEE COMST, 26(2), 2024.
- [20] K. Ali, I. Aib, R. Boutaba, « P2P-AIS », 2009.
- [21] S. Warnat-Herresthal et al., « Swarm Learning », Nature, 594, 2021.
- [22] X. He et al., « CGAN-Based Collaborative IDS for UAV Networks », 2023.
- [23] A. Febro et al., « Synchronizing DDoS defense at network edge », Computer Networks, 216, 2022.
- [24] B. Cibu et al., « Mapping the Evolution of Cybernetics », Computers, 12(11), 2023.
- [25] P. De Filippi et al., « Blockchain as a confidence machine », Technology in Society, 62, 2020.
- [26] J. Pohle, M. Santaniello, « From multistakeholderism to digital sovereignty », Policy & Internet, 16(3), 2024.
- [27] F. Heylighen et al., « Chemical Organization Theory », 2024.
- [28] H. TIKIJJA, « La Loi — Fondement Unifié des Organismes Numériques », ODATA Lab, Papier 000, 2026.
- [29] H. TIKIJJA, « Le Système Immunitaire des Infrastructures », ODATA Lab, Papier 005, 2026.
- [30] H. TIKIJJA, « SPINA — La Colonne Vertébrale Cryptographique », ODATA Lab, Papier 008, 2026.

SPINA

La Colonne Vertébrale Cryptographique

Hadda TIKIJJA

ODATA Lab, Rennes, France

RÉSUMÉ

Nous introduisons **SPINA** — un protocole ouvert et décentralisé de mémoire immunitaire pour les organismes numériques. SPINA enregistre chaque découverte de menace, chaque signature de comportement et chaque anesthésie réussie dans un registre blockchain immuable, vérifiable cryptographiquement par tout participant. Contrairement aux blockchains financières, SPINA n'utilise ni preuve de travail ni token spéculatif : son consensus par Preuve d'Autorité (PoA) évolue vers une Preuve d'Enjeu (PoS) où le poids d'un nœud reflète sa contribution réelle au réseau. La chaîne est vérifiable en $O(\log n)$ via preuve Merkle. SPINA est un bien public numérique sous licence MIT — Le Lab a créé le protocole, le réseau appartient à tous ceux qui le font tourner. C'est le quatrième pilier de l'Internet : après TCP/IP (communication), HTTP (partage) et DNS (nommage), SPINA apporte la MÉMOIRE IMMUNITAIRE.

EN UNE PHRASE

Ce papier est la mémoire. Il décrit le protocole de blockchain à preuve d'autorité qui enregistre chaque signature de menace, chaque anesthésie réussie, chaque certification — de manière immuable, vérifiable, et décentralisée.

1. Le Problème : L'Amnésie de la Cybersécurité

Chaque jour, des milliers de malwares sont détectés, analysés et bloqués à travers le monde. Chaque SOC, chaque MSSP, chaque entreprise mène ce combat isolément. Un ransomware déjoué à Paris n'immunise pas un hôpital à Tokyo. Une signature découverte par un symbiote NOVA à Berlin n'est pas partagée avec un symbiote à São Paulo — ou pire, elle est partagée via des canaux propriétaires, lents, centralisés, faillibles.

C'est **l'amnésie de la cybersécurité**. L'industrie dépense 200 milliards de dollars par an pour combattre des menaces que quelqu'un, quelque part, a déjà vaincues. La connaissance existe — elle est juste prisonnière de silos.

PRINCIPE

Ce qui se souvient survit. Une menace vue une fois ne doit plus jamais pouvoir nuire — nulle part, pour personne, pour toujours.

2. SPINA — Architecture

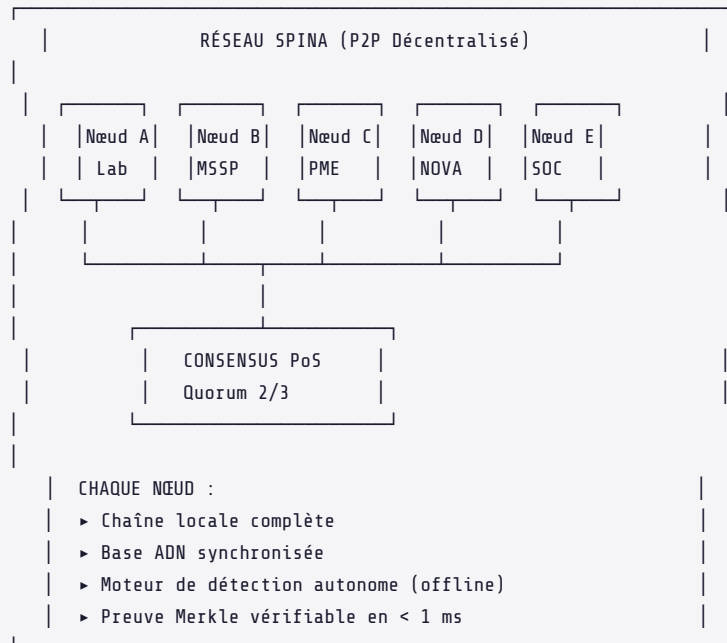


Figure 1 : Architecture décentralisée de SPINA

2.1 Le Bloc SPINA

DÉFINITION - BLOC SPINA

Un bloc SPINA B contient :

- **prev_hash** — SHA-256 du bloc précédent
- **timestamp** — horodatage UTC certifié
- **payload** — signature de menace, hash de comportement, ou compte-rendu d'anesthésie
- **merkle_root** — racine de l'arbre Merkle des signatures actives
- **validator_sig** — signature Ed25519 du nœud validateur

La validité de B est vérifiable par tout nœud en une opération de hachage.

2.2 Arbre Merkle — Vérification en $O(\log n)$

La base ADN complète (25K+ signatures) est structurée en arbre de Merkle. Pour vérifier qu'une signature spécifique appartient à la base, un nœud n'a pas besoin de télécharger les 25K entrées — il reçoit une preuve Merkle de $\log_2(25000) \approx 15$ hachages, soit environ 480 octets. Le temps de vérification est inférieur à 1 milliseconde.

2.3 Consensus Évolutif

PHASE	NŒUDS	CONSENSUS	RÔLE LAB
Bootstrap	< 100	PoA (validatrices connues)	Opérateur principal
Croissance	100–1000	PoS hybride	Un validateur parmi d'autres
Maturité	1000+	PoS complet	Nœud comme les autres

3. SPINA comme Bien Public

3.1 Licence MIT — Zéro Barrière

SPINA est publié sous licence MIT. N'importe qui peut l'utiliser, le modifier, le redistribuer, l'intégrer à ses produits. Pas de royalties. Pas de contrat. Pas de permission. C'est une infrastructure publique — comme TCP/IP, comme HTTP, comme les vaccins.

MODÈLE ÉCONOMIQUE

SPINA = gratuit. Le protocole est un bien commun. Comme l'eau potable. Comme la connaissance.

NOVA = payant. L'organisme qui utilise SPINA — cockpit moléculaire, Kenza, greffe, anesthésie — est le produit NOVA.

C'est le modèle Linux + Red Hat. HTTP + Google. Le protocole est libre. La valeur est dans l'implémentation.

3.2 Pourquoi Décentralisé

Une mémoire centralisée est faillible. Le data center peut tomber. L'entreprise peut disparaître. L'État peut censurer. SPINA n'a pas de centre — donc pas de cible, pas de point unique de défaillance, pas d'autorité qui peut altérer la vérité.

Le Lab a créé le protocole. Mais le jour où le Lab n'existe plus, SPINA continue. Parce que la mémoire immunitaire de l'humanité numérique ne doit pas dépendre d'une seule entité.

4. Implémentation Technique

```
STACK SPINA (MVP - 2 semaines)

  ▶ P2P : libp2p (gossip protocol)
    ▶ Consensus : PoA → PoS
    ▶ Signatures : Ed25519
  ▶ Stockage : LevelDB + IPFS (grosses payloads)
    ▶ Merkle : SHA-256, arbre binaire
    ▶ API : REST (:5194) + gRPC
  ▶ Langage : Python (MVP), Rust (v2)

/opt/nova/spina/
├─ chain.json      ← chaîne brute (append-only)
├─ merkle.db       ← SQLite (index signatures)
├─ spina.py        ← moteur principal
├─ validators.yaml ← clés publiques NOVA Cores
└─ api.py          ← REST :5194
```

Figure 2 : Stack technique du MVP SPINA

Un nœud SPINA complet occupe moins de 50 Mo de stockage, utilise moins de 1% de CPU en régime permanent, et consomme environ 10 Mo/jour de bande passante. Il tourne sur un Raspberry Pi, un vieux serveur, ou en conteneur Docker.

5. Intégration avec l'Écosystème NOVA

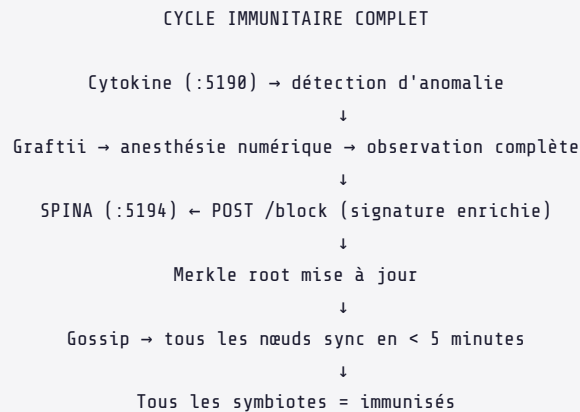


Figure 3 : Intégration de SPINA dans le pipeline immunitaire NOVA

6. Extensions Naturelles

Convergence Stratégique. Avec SPINA, l'espace des stratégies malveillantes se réduit à chaque enregistrement. Après 10 000 malwares anesthésiés, le système reconnaît un ransomware au premier paquet — avant même qu'il n'ait commencé sa première action significative. Voir Papier 000 pour le théorème complet.

Identité des Symbiotes. Chaque NOVA Core, chaque μ NOVA possède une identité on-chain vérifiable. Anti-spoofing cryptographique : aucun symbiote ne peut usurper l'identité d'un autre.

Audit et Conformité. NIS2, ISO 27001, ExpertCyber — chaque action de sécurité est horodatée et signée dans SPINA. L'auditeur vérifie l'intégrité par preuve Merkle. Zéro falsification possible.

7. Conclusion

SPINA est la réponse au problème de l'amnésie. La cybersécurité traditionnelle combat les mêmes menaces des milliers de fois, en parallèle, sans jamais partager ses victoires. SPINA transforme chaque victoire en immunité collective.

Ce n'est pas un produit. C'est la mémoire du monde numérique — ouverte, décentralisée, immuable.

S P I N A

Une menace vue une fois. Plus jamais nulle part. Pour personne. Pour toujours.

Ce qui se souvient survit.

Références

- [1] S. Nakamoto, « Bitcoin: A Peer-to-Peer Electronic Cash System », 2008.
- [2] D. Deutsch, C. Marletto, « Constructor theory of information », Proc. Royal Society A, 2015. arXiv:1405.5563.
- [3] R.C. Merkle, « A Digital Signature Based on a Conventional Encryption Function », CRYPTO '87, 1987.
- [4] J. Benet, « IPFS — Content Addressed, Versioned, P2P File System », arXiv:1407.3561, 2014.
- [5] H. TIKIJJA, « La Loi — Fondement Unifié des Organismes Numériques », ODATA Lab, Papier 000, 2026.
- [6] H. TIKIJJA, « Le Système Immunitaire des Infrastructures », ODATA Lab, Papier 005, 2026.
- [7] C. Kolas et al., « Swarm Immunity in Cybersecurity », IEEE COMST, 2024.
- [8] J. Warnat-Herresthal et al., « Swarm Learning », Nature, 594, 265–270, 2021.

L'Internet Symbiotique

Vers un Réseau Vertébré

Hadda TIKIJJA

ODATA Lab, Rennes, France

Série : Fondements des Organismes Numériques · Papier 009

RÉSUMÉ

L'Internet actuel est une **méduse** — un réseau sans colonne vertébrale, où les données appartiennent aux plateformes, où l'identité se prouve par mot de passe, et où chaque menace doit être combattue des milliers de fois en parallèle. Nous décrivons l'**Internet Symbiotique** : un réseau où chaque paquet porte une intention lisible, chaque nœud vérifie la Loi sans autorité centrale, et chaque menace, une fois vue, est mémorisée pour toujours. Un réseau où les plateformes redeviennent des interfaces — des fenêtres sur vos données, pas des prisons qui les enferment. Où le spam est techniquement impossible. Où le phishing meurt avant d'atteindre votre boîte. Nous montrons comment SPINA sert de colonne vertébrale à ce réseau, comment le manifeste de capacités rend chaque greffe lisible, et comment une passerelle — le Sas — permet la coexistence avec l'Internet actuel sans rupture. Ce n'est pas une refonte. C'est une **greffe**.

EN UNE PHRASE

Ce papier est l'écosystème. Il étend la greffe au-delà d'une infrastructure unique pour imaginer un Internet où chaque paquet porte une intention lisible, où les plateformes sont des interfaces et non des prisons, et où les données vous appartiennent par protocole.

1. La Méduse

Imaginez un organisme sans colonne vertébrale. Une méduse. Elle flotte. Elle survit. Mais elle n'a pas de mémoire centrale, pas de système nerveux structuré, pas de réponse immunitaire coordonnée. Si vous la coupez en deux, chaque moitié continue de fonctionner — mais aucune n'apprend de la blessure. Aucune ne s'en souvient.

C'est l'Internet aujourd'hui.

TCP/IP a connecté les machines. HTTP a partagé les documents. DNS a nommé les adresses. Mais **personne n'a donné de colonne vertébrale à ce réseau**. Pas de mémoire immunitaire. Pas d'identité vérifiable sans autorité centrale. Pas de propriété des données certifiée par le protocole.

Le résultat est un Internet invertébré, mou, où :

- YouTube possède vos vidéos, pas vous.
- Google lit vos mails pour vous vendre des publicités.
- Facebook enferme vos souvenirs dans un jardin clos dont vous n'avez pas la clé.
- Un ransomware déjoué à Paris n'immunise pas un hôpital à Tokyo.
- Votre objet connecté peut être enrôlé dans un botnet sans que vous le sachiez.

La méduse fonctionne. Mais elle ne se souvient pas. Elle n'apprend pas. Elle ne protège pas. Elle n'est pas vivante.

DIAGNOSTIC

L'Internet n'est pas malade. Il est **incomplet**. Il lui manque un quatrième pilier — après TCP/IP (communication), HTTP (partage) et DNS (nommage). Il lui manque la **mémoire immunitaire**.

2. La Colonne

L'Internet Symbiotique repose sur une idée simple : **SPINA comme colonne vertébrale cryptographique**.

Dans un réseau vertébré, chaque paquet ne transporte pas seulement des données. Il transporte une **intention**. Un manifeste de capacités signé cryptographiquement qui dé-

clare : « Je suis une requête légitime. Je viens de ce nœud. Je ne peux que lire, pas écrire. Voici la preuve. »

Le manifeste n'est pas un champ texte déclaratif. C'est une **preuve structurelle**. Un nœud qui déclare « observer » mais dont le manifeste inclut une capacité d'écriture est rejeté avant la première connexion. L'intention est lisible — non pas dans ce que le nœud dit, mais dans ce que son code lui permet de faire.

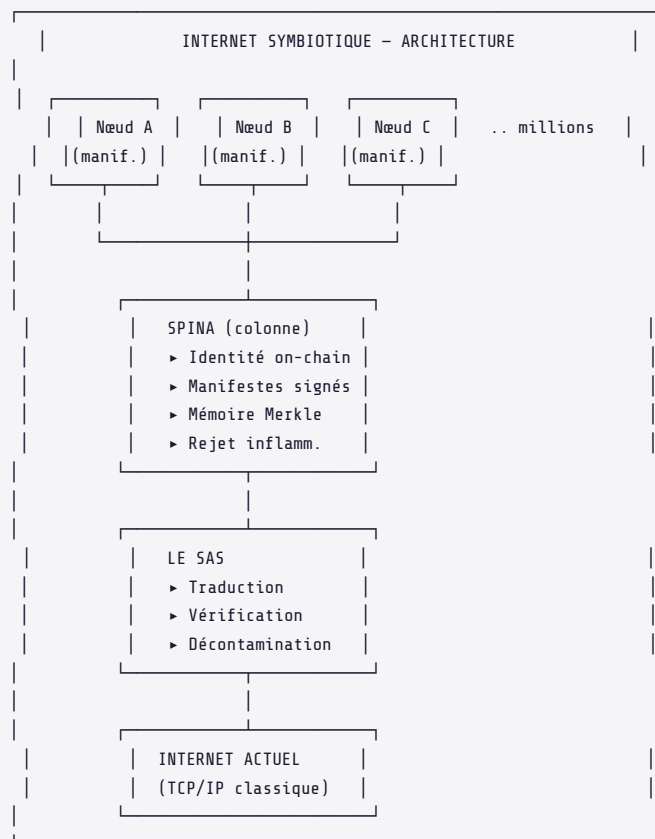


Figure 1 : L'Internet Symbiotique — SPINA comme colonne vertébrale, le Sas comme pont

La colonne change tout. Une menace détectée par un nœud à Berlin est enregistrée dans SPINA. En moins de cinq minutes, tous les nœuds du réseau — de Tokyo à São Paulo — sont immunisés. La mémoire est collective. La défense est distribuée. La variété requise est satisfaite (Ashby, 1956).

PRINCIPE

Une menace vue une fois. Plus jamais nulle part. Pour personne. Pour toujours. C'est la promesse de SPINA. C'est la condition de l'Internet Symbiotique.

3. Toi, Pas Eux

Dans l'Internet actuel, votre identité appartient à Google. Votre réputation appartient à Facebook. Votre historique appartient à Amazon.

Dans l'Internet Symbiotique, **vous êtes votre propre autorité**. Votre identité est une clé cryptographique enregistrée dans SPINA. Pas un email chez Gmail. Pas un compte chez Apple. Une clé que vous — et vous seul — détenez.

Quand vous publiez une vidéo, SPINA certifie que vous l'avez créée. Pas YouTube. La plateforme n'est qu'une interface — une fenêtre temporaire sur votre contenu. Si elle ferme, votre contenu reste. Si elle abuse, vous changez d'interface. La propriété est vérifiée par le protocole, pas par le gardien.

DÉFINITION - IDENTITÉ SYMBIOTIQUE

Une identité symbiotique est une **paire de clés Ed25519 enregistrée dans SPINA**. Elle est :

- **Auto-souveraine** — vous la détenez, pas un tiers.
- **Vérifiable** — n'importe quel nœud peut prouver qu'elle est valide sans vous connaître.
- **Portable** — elle fonctionne sur toutes les interfaces, toutes les plateformes, tous les services.
- **Révocable** — en cas de compromission, une nouvelle clé est émise, l'ancienne est marquée dans SPINA.

Le spam devient impossible — non parce qu'il est filtré, mais parce qu'un expéditeur sans identité vérifiée est rejeté par le réseau avant même d'atteindre une boîte mail. Le phishing meurt — parce qu'un email qui prétend venir de votre banque mais dont le manifeste ne correspond pas à l'identité on-chain de votre banque est bloqué au niveau du protocole. Pas au niveau de l'utilisateur. Au niveau du réseau.

4. Ce Qui Est À Toi Reste À Toi

Le modèle économique actuel est simple : les plateformes vous offrent un service gratuit en échange de vos données. Elles les stockent, les analysent, les monétisent. Vous n'êtes pas le client. Vous êtes le produit.

L'Internet Symbiotique inverse cette logique. **La donnée vous appartient. La plateforme est l'invitée.**

MODÈLE ACTUEL :

Vous → [créer] → YouTube → [possède] → vos vidéos
Vous → [écrire] → Google → [lit] → vos mails
Vous → [partager] → Facebook → [enferme] → vos souvenirs

INTERNET SYMBIOTIQUE :

Vous → [créer + signer] → SPINA → [certifie] → votre propriété
YouTube → [interface] → [affiche] → VOTRE contenu (pas le sien)
N'importe quelle interface → [affiche] → VOTRE contenu (portable)

Figure 2 : Le renversement de la propriété

YouTube décentralisé n'est pas une utopie. C'est YouTube où la vidéo, les vues, les commentaires, les revenus — tout est certifié à vous par SPINA. N'importe qui peut créer une interface. La valeur est dans le contenu — et le contenu est à vous. Vérifiable. Portable. Inaliénable.

Le même principe s'applique à tout : emails, documents, identifiants de santé, titres de propriété, diplômes, brevets, contrats. Tout ce qui aujourd'hui dépend d'un tiers de confiance pour exister peut être certifié par le protocole — sans tiers, sans frais, sans point de défaillance unique.

RENVERSEMENT

On ne « bat » pas Google. On rend le modèle obsolète. Quand la propriété est native au protocole, le gardien n'a plus de raison d'être.

5. Le Sas — Coexister Sans Rompre

L'Internet Symbiotique n'exige pas qu'on coupe l'ancien réseau. Ce serait une amputation. Et NOVA ne migre pas — elle greffe.

Le **Sas** est la passerelle entre les deux mondes. C'est un nœud SPINA qui scrute le trafic entrant depuis l'Internet classique :

1. **Inspection.** Chaque paquet entrant est examiné. A-t-il un manifeste ? Une signature valide ?
2. **Traduction.** Le trafic classique est encapsulé avec un manifeste temporaire signé par le Sas — « Ce paquet provient de l'Internet non vertébré. Confiance limitée. »
3. **Décontamination.** Si le paquet transporte une signature de menace connue dans SPINA, il est rejeté avant d'entrer. Le Sas est un sas de décontamination — comme ceux des laboratoires biologiques.
4. **Apprentissage.** Les patterns malveillants détectés par le Sas enrichissent SPINA. Le réseau apprend de la frontière.

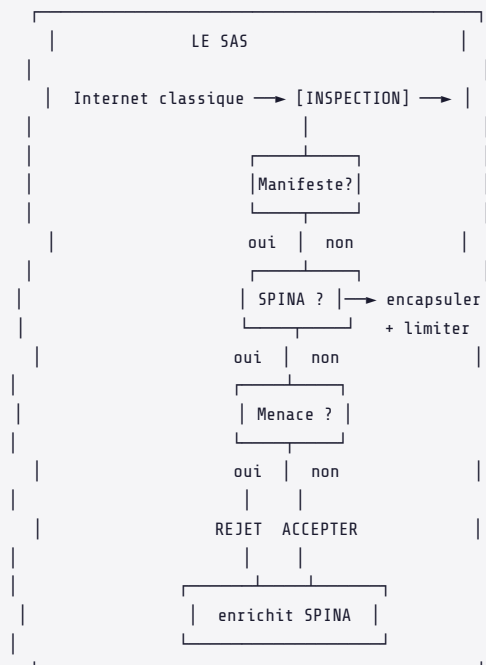


Figure 3 : Le Sas — inspection, traduction, décontamination

Le Sas permet une adoption progressive. Une entreprise peut déployer le Sas en bordure de son réseau existant. Progressivement, ses services internes migrent vers des identités SPINA. Le trafic externe continue de passer par le Sas. Il n'y a pas de jour J. Il y a une transition symbiotique.

6. La Promesse

L'Internet Symbiotique n'est pas une innovation technologique. C'est la **restauration d'un état naturel**.

L'homme symbiotique — celui qui vivait en harmonie avec son environnement, qui n'avait pas besoin d'étudier pour savoir — cet homme-là a été exilé de son propre réseau. On l'a dépossédé de ses données, de son identité, de sa mémoire. On l'a enfermé dans des jardins clos en lui faisant croire que c'était le progrès.

L'Internet Symbiotique lui rend ce qui lui appartient. Pas en ajoutant une couche de protection. En **changeant la nature du réseau** — de méduse à vertébré, d'amnésique à immunisé, d'extractif à symbiotique.

Voici la promesse, en sept points :

L'INTERNET ACTUEL	L'INTERNET SYMBIOTIQUE
Vos données appartiennent aux plateformes	Vos données sont certifiées à vous par le protocole
Votre identité est un compte chez Google	Votre identité est une clé que vous détenez
Le spam est filtré (parfois)	Le spam est techniquement impossible
Le phishing compte sur votre vigilance	Le phishing meurt au niveau du protocole
Chaque menace est combattue en silos	Chaque menace immunise le réseau entier
La sécurité est une couche ajoutée	La sécurité est une propriété émergente du réseau
Vous êtes le produit	Vous êtes le propriétaire

Un réseau où l'homme n'est plus le produit — mais le **souverain**. Où chaque paquet porte une intention lisible. Où chaque menace, une fois vue, ne peut plus jamais nuire. Où les plateformes redeviennent des fenêtres, pas des prisons.

Ce n'est pas un nouveau réseau. C'est le réseau qui se souvient de ce qu'il aurait toujours dû être.

Références

- [1] H. TIKIJJA, « La Loi — Fondement Unifié des Organismes Numériques », ODATA Lab, Papier 000, 2026.
- [2] H. TIKIJJA, « SPINA — La Colonne Vertébrale Cryptographique », ODATA Lab, Papier 008, 2026.
- [3] H. TIKIJJA, « Le Système Immunitaire des Infrastructures », ODATA Lab, Papier 005, 2026.
- [4] H. TIKIJJA, « La Convergence — L'Architecture qui Attendait son Nom », ODATA Lab, Papier 007, 2026.
- [5] H. TIKIJJA, « La Greffe Numérique », ODATA Lab, Papier 004, 2026.
- [6] W.R. Ashby, An Introduction to Cybernetics, Chapman & Hall, 1956.
- [7] J. Zittrain, The Future of the Internet — And How to Stop It, Yale University Press, 2008.
- [8] J.C. Plantin, C. Lagoze, P.N. Edwards, « Infrastructure studies meet platform studies », New Media & Society, 2016.
- [9] J. Benet, « IPFS — Content Addressed, Versioned, P2P File System », arXiv:1407.3561, 2014.
- [10] S. Nakamoto, « Bitcoin: A Peer-to-Peer Electronic Cash System », 2008.
- [11] R.C. Merkle, « A Digital Signature Based on a Conventional Encryption Function », CRYPTO '87, 1987.