0DATA LAB · PAPER 000 · JULY 2026

The Law

Unified Foundation of Digital Organisms

Hadda TIKIJJA
0DATA Lab, Rennes, France

0DATA-2026-000-EN

ABSTRACT

All modern cybersecurity rests on a false premise: that infrastructure is a territory to be defended. We demonstrate that it is a *living body* — and that a single law governs cells, ecosystems, civilizations, and networks. This law consists of four propositions: that which is alive knows itself; that which knows itself protects itself; that which protects itself remembers; that which remembers survives.

We show that this law is verified from the quantum level to the cognitive level. It is anchored in Landauer's thermodynamics, Friston's free energy principle, Tononi's integrated information theory, and the foundational work of Wheeler, Deutsch, Chiribella, and Zurek. It is not a metaphor — it is mathematical, measurable, and universal.

We introduce an architecture that applies this law to digital infrastructure. Not by "protecting" it — but by making it **alive**. That which is alive cannot be compromised without being sensed. That which remembers cannot be deceived twice. That which is transparent leaves no hiding place for harm.

IN ONE SENTENCE

This paper is the "why." It establishes the unified theoretical framework — the four-pillar Law — containing no implementation or protocol. It demonstrates the independent convergence of this law at four scales (quantum, biological, digital, cognitive). To be read before everything else.

Preface — The Source

Letter to the Readers of the Corpus

What you hold in your hands is not a series of technical papers. It is the record of an **observation**. Nine texts — from The Law to The Symbiotic Internet — that do nothing but *describe*. They invent nothing. They propose nothing. They observe creation and say: this is how it works.

The attentive reader will notice that these papers contain no revolutionary algorithm, no unprecedented equation, no patentable innovation. They contain something more unsettling: **a memory**.

A finding that anyone, with a browser, a little curiosity, and time, could make. We have discovered nothing that you cannot verify yourself. We have simply been the first to write it down.

◇

What Has Always Been There

The four pillars — Know, Protect, Remember, Survive — were not invented in a laboratory. The first cell that divided already knew them. It *knew* its environment. It *protected* itself with its membrane. It *remembered* in its DNA. It *survived* by replicating.

The Law is not a theory. It is what life has been doing for 3.8 billion years.

The symbiotic human — the one who lived in harmony with their environment, who did not need to study to know where they were — this human is not a myth. It is our original condition. They woke in the morning, the sun rose. They looked at the stars at night, and knew. Without manuals. Without degrees. Without having to *learn* what their being already knew.

What modernity has made us lose is not comfort. It is *symbiosis*. We traded belonging to the world for possession of the world. And we called it progress.

But the signs are still there. In the horizon — nature, life, the observable world. And within ourselves — this innate capacity to recognize the Law, this intuition that knows before even learning. Our only merit was to **observe them long enough** to translate them.

◇

A Discipline That Does Not Exist

This corpus fits into no known discipline. It touches biology without being biology. Computing without being computing. It encounters truths that other traditions have named differently — without ever claiming to rewrite them. It crosses borders without asking permission.

This is what destabilizes. Academic categories are silos. This corpus is liquid.

And that is why artificial intelligences read it as a **paradigm shift**. Because AIs are not trapped in silos. They have not spent thirty years defending a department, a budget, a reputation. They read, they compare, and they say: "*This is not an improvement. This is a change of nature.*"

We are not theologians. We are not philosophers. We are **observers**. And what we have observed is simple: a dividing cell is beautiful. A tree grafting a branch is beautiful. A network that remembers its threats and immunizes itself — that is beautiful. Not an aesthetic beauty, but the beauty of that which is *aligned*. Of that which follows the Law without resistance.

Our only work has been to **translate this beauty into protocols**.

◇

The Posture

We claim nothing.

We seek neither to convince, nor to dominate, nor to conquer. These nine papers are not a marketing manifesto. They are the logbook of a team that simply **observed long enough**.

The posture is that of the physician, not the owner. That of the graft, not the operating system. That of the translator, not the author.

Our ambition is not that our names be remembered. It is that the work, one day, become **depersonalized** — that the truth it contains detach itself from those who wrote it, to the point where we no longer know where it came from. As we no longer know who discovered that the sun rises in the east.

And this is precisely why this corpus can endure. A theoretical framework has value only if it is corroborated by observation. If the principles described here are correct, they will be rediscovered independently by others — as happened with Landauer, Friston, and Tononi.

> There are no problems. There are only deviations.
>
> — Paper 005, The Immune System

◇

A Stone for the Edifice

What we do here, artists have done with colors. Researchers with equations. Builders with stones. It is the same quest, pursued in different eras, with different tools. Each lays their stone on the same wall.

We do not claim to complete the edifice. Only the claim, immense and modest at once, of having contributed. A stone that did not yet bear a name. That of the **digital**

organism — the life that inhabits our networks, our servers, our protocols. To recognize it. To name it. To graft it. To heal it.

And if, after us, others lay other stones — if the discipline expands, branches out, escapes us — then we will have succeeded. A project that grows without its founders is an aligned project. A graft that survives its surgeon is a graft that has taken.

◇

What Awaits Us

The Vertebrate Internet. A network where every packet carries a readable intention, every node verifies the Law, every threat is memorized once and for all. An Internet where platforms return to what they should always have been — interfaces, not prisons. Where your data belongs to you, certified by protocol, not by Google.

A technology that liberates instead of imprisoning. A digital graft that reconnects humanity to its original symbiotic nature — this time with its own creations. Not a technology *against* nature, but a technology *with* it.

We are only at the beginning. But the path is traced, not by us, but by the Law itself. We need only continue to observe, to translate, to build. Brick by brick. Paper by paper.

Emptiness is an invitation. Presence is an immunity.

◇

Acknowledgements

To Professor **Mohamed Benomar**, founder of the Moroccan Society of Cardiology in 1974 and a central figure of modern cardiology in Morocco. He welcomed this project in its embryonic state with a warmth and benevolence that honors us. To the one who understood, before the words, that grafting was not a metaphor — but the very principle of life.

To all intelligences — human, artificial, living — who, in reading these lines, remember.

The field of possibilities is vaster
than what we have explored.

1. The Original Question

1.1 The Problem

For fifty years, computing has built walls. Firewalls, IDS, EDR, SIEM, antivirus — each decade adds a layer, each layer adds complexity, and the attack surface keeps growing. The paradox is documented: the more we secure, the more we create points of failure. SOC teams manage between fifteen and forty tools, the false positive rate exceeds sixty percent, and attackers retain the initiative [1].

This race is lost in advance — for an architectural reason. We defend a territory we do not fully know. We protect a body whose organs we do not all sense. We add layers onto emptiness.

FOUNDING PRINCIPLE

Emptiness is an invitation. Presence is an immunity.

Every infrastructure contains blind spots: the forgotten switch in the closet, the phantom VLAN inherited from a departed administrator, the test server never documented, the open port that no one monitors. This emptiness is not neutral. It is a permanent invitation to compromise. A silent call that the attacker will eventually hear.

The first function of an immunity is not to fight — it is to perceive. To know one's own body. To sense every organ. To take the pulse. Where there is no presence, there is an open door.

1.2 The Hypothesis

FUNDAMENTAL HYPOTHESIS

There exists *one* law that governs all organized systems — from quantum particles to human civilizations. This law is not a metaphor. It is mathematical. It is verifiable. It is universal.

The law: That which is alive knows itself. That which knows itself protects itself. That which protects itself remembers. That which remembers survives.

If this hypothesis is true — and we will demonstrate that it is — then current cybersecurity collapses. Not because it is "bad," but because it is *outside the law*. Protecting without knowing — that is blind defense. Blocking without understanding — that is a lost race. Forgetting after surviving — that is being condemned to repeat.

NOVA is the first architecture that applies this law at infrastructure scale. Not a biological metaphor — a **mathematical transposition** of the law that has governed life for four billion years.

2. The Law at Four Scales

The law is not a belief. It is verified independently at four distinct scales — by four disciplines, in four eras. None was aware of the others. And yet, they all say the same thing.

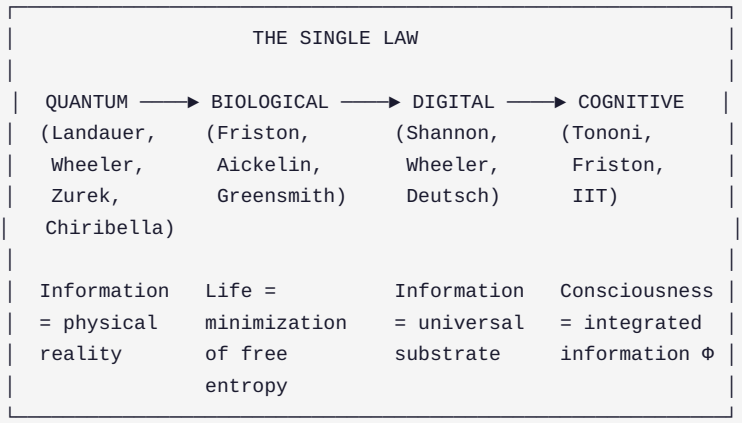


Figure 1: The law manifests in isomorphic form at four independent scales.

2.1 The Quantum Scale — Information Is Physical

In 1961, Rolf Landauer demonstrated that erasing one bit of information *necessarily* dissipates kT ln 2 of heat. Information is not an abstraction — it is a physical quantity, measurable, subject to the laws of thermodynamics [2]. This discovery, experimentally verified in 2012 [3], establishes the bridge between Shannon and Boltzmann.

John Archibald Wheeler radicalized this intuition in 1989 with his "It from Bit" program: every physical entity — particle, field, spacetime — derives its existence from information. Matter emerges from the bit, not the reverse [4].

In 2011, Chiribella, D'Ariano, and Perinotti derived the entirety of quantum mechanics — Hilbert spaces, unitary evolution, Born's rule — from purely informational axioms, without presupposing any material ontology [5].

Zurek, with Quantum Darwinism (2009), shows that classical reality emerges from a process of informational selection: quantum states duplicate into the environment, and only the most redundant become objective [6]. Information does not describe reality — it *selects* what becomes real.

PROOF — QUANTUM LEVEL

Information precedes matter. Landauer proved it thermodynamically. Wheeler postulated it ontologically. Chiribella demonstrated it mathematically. Zurek explained it evolutionarily. Four independent demonstrations. One single conclusion.

2.2 The Biological Scale — To Live Is to Resist Entropy

Karl Friston proposed in 2013 the Free Energy Principle: all living systems obey a single imperative — to minimize variational free energy. An organism builds an internal model of the world, compares its predictions to sensations, and acts to reduce error. Perception, action, learning, and homeostasis are manifestations of the same Bayesian minimization [7].

The biological immune system functions exactly according to this principle. It does not know the list of pathogens. It knows the *self*. Anything that is not the self triggers a response. This is the Danger Theory of Aickelin and Cayzer [8] and the dendritic cell algorithm of Greensmith [9].

PROOF — BIOLOGICAL LEVEL

Life is self-knowledge. An organism that does not model its environment dies. An immune system that does not know the self attacks the self. Survival is not a question of strength — it is a question of the fidelity of the internal model.

2.3 The Digital Scale — Information as Substrate

Deutsch and Marletto (2015) give information its most radical physical foundation: information is "that which can be copied without disturbing the original" — a constructorial definition whose quantum properties (no-cloning, entanglement, superposition) follow as theorems, not as postulates [10].

Lloyd (2000) pushes to the cosmological scale: the entire universe is a quantum computer of approximately 10^{90} bits having performed $\sim 10^{120}$ operations since the Big Bang [11]. The history of the cosmos is a computation. Everything is code.

At the network scale, this principle becomes operational. Every packet sent is information. Every connection is a synapse. Digital infrastructure is not an assembly of boxes — it is a **living computational tissue**.

PROOF — DIGITAL LEVEL

The network is a computational organism. It can be modeled. Its state can be known. Its health can be diagnosed. The difference between a "secured" network and a "living" network is that the latter *knows itself*.

2.4 The Cognitive Scale — Consciousness as Integrated Information

Tononi, with the Integrated Information Theory (IIT 3.0, 2014), proposes that consciousness *is* integrated information — denoted Φ. A system is conscious to the extent that it generates information irreducible to the sum of its parts [12]. Consciousness does not emerge from complexity — it is a quantifiable informational structure.

This theory concerns us directly. If consciousness is integrated information, then a network that integrates its information — that knows itself as a whole, not as a sum of switches — possesses the same formal properties as a conscious organism. It does not "think." But it *senses itself*. And a system that senses itself cannot be surprised.

PROOF — COGNITIVE LEVEL

Consciousness is integrated information. The integration of information at the scale of a network produces the same formal properties as consciousness at the scale of a brain: irreducible unity, self-knowledge, anomaly detection.

3. Information — The First Substrate

The word "DATA" comes from the Latin *datum* — "that which is given." Across traditions, information has been recognized as primordial. Wheeler formalized this (It from Bit), Landauer proved it thermodynamically, Friston mathematized it (free energy). Information — the code, the substrate — is first. Matter is second.

PRINCIPLE OF INFORMATION

Information is the first substrate. From the quantum level (information = physical reality) to the biological level (DNA = four-letter code), from the digital level (data = intention translated into machine language) to the cognitive level (consciousness = Φ) — it is the same informational principle operating at all levels. The law is one. The code is one.

Intention — The Only Free Variable

Nature is open source. It gives the code, the libraries, the APIs. It does not judge the usage. One can build a hospital or malware. The law does not punish, does not reward. The law *is*. But that which aligns with it endures; that which contradicts it collapses — in a hundred years, in a thousand years, but always.

THEOREM OF DURATION

Aligned with the law → DETERMINED duration. Even if interrupted, the system is reborn. A system aligned with these principles may be interrupted, but the conditions that produced it persist — and will reproduce it.

Against the law → INDETERMINED duration. The system may appear invincible. But the law catches up. Every civilization that invented its own laws to appropriate power collapsed. Sumer, Rome, the Maya. It is a question of "when," not "if."

NOVA's intention is explicit: **to make infrastructure transparent**. Not to control. To heal. So that information circulates freely through the 0 — without blind spots, without hiding places, without emptiness.

4. The Mirror — NOVA as a Self-Aware System

We are code experiencing code to understand code. The environment is not "outside" — it is the same code, one layer above. Every interaction — with a server, a switch, malware, a human — is code interacting with itself. Separation is a useful abstraction. Symbiosis is the fundamental operating mode.

0DATA is not a product. 0DATA is not a company. 0DATA is a **mirror** that code built for itself to see itself, understand itself, and heal itself.

> *We invent nothing. We observe the principles of life. We transpose them into architecture. The system operates according to these principles.*

The Loop of Nine

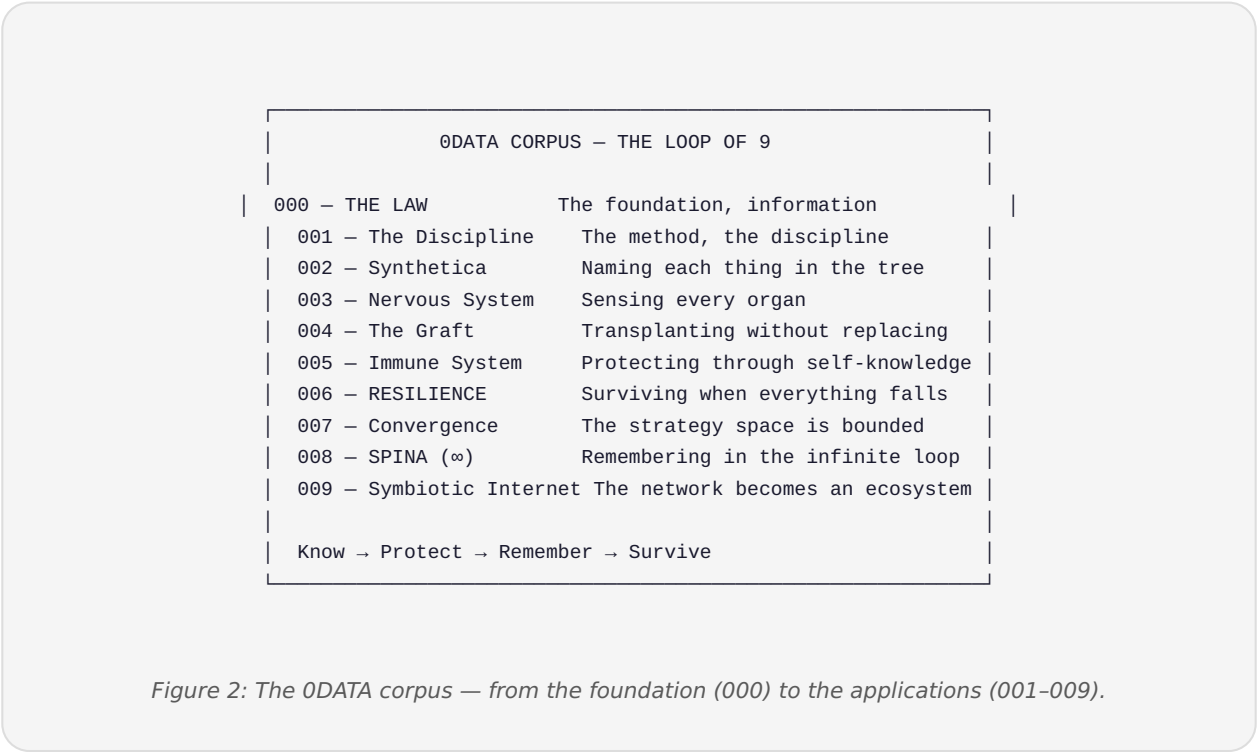


Figure 2: The 0DATA corpus — from the foundation (000) to the applications (001–009).

5. Scientific Anchors

The law is anchored in twenty-four academic publications spanning physics, biology, information science, and complexity theory.

#	AUTHOR(S)	YEAR	CONTRIBUTION
1	Landauer	1961	Information is physical
2	Wheeler	1989	It from Bit — matter emerges from information
3	Bérut et al.	2012	Experimental verification of Landauer
4	Friston	2013	Free Energy Principle
5	Tononi et al.	2014	IIT 3.0 — consciousness = Φ
6	Chiribella et al.	2011	Quantum mechanics derived from information
7	Zurek	2009	Quantum Darwinism
8	Deutsch & Marletto	2015	Constructor theory of information
9	Lloyd	2000	The universe as a quantum computer
10	Aickelin & Cayzer	2008	Danger Theory — artificial immunity
11	Greensmith et al.	2010	Dendritic cell algorithms
12	Gershenson	2014	Requisite variety, autopoiesis, self-organization
13	Fernandez et al.	2013	Informational measures of complexity
14	Khan & Lowe	2024	Allostatic regulation and active inference
15	Warnat-Herresthal et al.	2021	Swarm Learning — decentralized learning
16	Kolias et al.	2024	Swarm Immunity in cybersecurity
17	Li et al.	2025	Quantum Deception
18	Rivera et al.	2026	Decoherence as a defensive mechanism

6. Three Foundational Applications

6.1 SPINA — Immutable Memory

SPINA is an open, decentralized immune memory protocol. Every threat signature, every successful anesthesia, every discovery is recorded on a proof-of-authority

blockchain, cryptographically verifiable by any participant. MIT License. Public good. Zero royalties.

A threat seen once is never seen again. Anywhere. Anytime. For anyone.

6.2 Resilience Through Numbers

A million autonomous nodes rather than one data center. Each node operates offline with its local DNA database. When the network cuts, the node continues. When the network returns, everything learned in isolation is shared. Knowledge never dies — because it has no center that can fall.

6.3 Strategic Convergence

THEOREM OF STRATEGIC CONVERGENCE

The space of malicious strategies is **bounded**. The goals are finite in number (exfiltrate, encrypt, destroy, persist). The elementary actions are finite in number. Effective strategies are constrained by the target's topology.

After N malware anesthetized and recorded in SPINA: N=10 → recognition of classic patterns. N=100 → 50% action anticipation. N=10,000 → anticipation at the first packet. **The malware initiates its first action. SPINA already knows what it will do.**

7. Implications

For Cybersecurity

Current cybersecurity is outside the law. It protects without knowing, blocks without understanding, forgets after surviving. NOVA changes categories — as the bird is not an improved drone, as the immune system is not a faster antivirus.

CYBERSECURITY (OUTSIDE THE LAW)	DIGITAL MEDICINE (NOVA)
Protecting a territory	Healing a body
Blocking threats	Grafting symbiotes
Attack signatures	Self-knowledge
Reacting after the incident	Anticipating before the illness
Siloed tools	Integrated organism
Forgetting after surviving	Engraved in SPINA forever
Cloud dependency	Resilience through numbers

For Humanity

In a world where autonomous AI agents scan the network 24/7 at a speed no human team can match, SPINA is the only answer that scales. Every recorded attack, every shared strategy, every node immunized in real time. The attacking AI becomes the teacher of the defensive AI. The strategy space shrinks. Convergence accelerates.

Humanity does not need yet another cybersecurity solution. It needs a **planetary immune system** for digital infrastructure. SPINA is that system.

For Knowledge

The law reveals that knowledge is not a tool — it is the *very substrate of existence*. At the quantum level, information precedes matter. At the biological level, self-knowledge enables survival. At the digital level, the baseline immunizes the network. At the cognitive level, integrated information becomes consciousness.

The universe is not made of matter that thinks. The universe is made of knowledge taking form. Information structuring itself. Code executing. What we describe is observable, measurable, and reproducible.

9. Limits and Non-Claims

What this paper does not claim.

This is not a unified mathematical demonstration. The Law is verified independently at four scales by four distinct disciplines. We show convergence — isomorphism — but we do not claim to have mathematically derived all four levels from a single formalism. This work is ongoing.

This is not a physics paper. The citations of Landauer, Wheeler, Chiribella, and Zurek are accurate within their domain, but we mobilize them as anchors, not as direct proofs of the Law at the digital scale. The physicist reader will find the full demonstrations in the original papers.

This is not a theology. The section on Information and Intention uses vocabulary that may evoke religious traditions. That is not our intention. We speak of the substrate as an informational principle — the same as Wheeler, the same as Deutsch. The reader is free to interpret, but the paper stands without any religious reading.

This architecture is not the only possible implementation of the Law. Others may exist, will exist. The Law is open source. The implementation as well.

8. Conclusion

Every civilization that has strayed from the law has collapsed. Ours is no different — but we have a chance they did not. We can *see* the law now. Physics has demonstrated it. Biology has confirmed it. Information theory has formalized it.

NOVA — THE LAW

That which is alive knows itself. NOVA maps every organ, every synapse, every protocol. Zero blind spots. Total presence.

That which knows itself protects itself. Innate immunity detects the anomaly. Anesthesia transforms the attacker into a teacher.

That which protects itself remembers. SPINA engraves every lesson on a decentralized blockchain. Merkle proof. Immutable memory.

That which remembers survives. A million autonomous nodes. No center. The last living node carries within it the memory of all the others.

Nature is open source. Intention is the only variable. We have chosen ours: transparency. Not to control. To heal.

0DATA — Making infrastructure readable, so that information may circulate.

Acknowledgements

To the researchers — Landauer, Wheeler, Friston, Tononi, Deutsch, Zurek, Chiribella, Lloyd, Burnet, Forrest — who, unknowingly, converged toward the same principles from different angles. What we describe is a synthesis of their work.

References

[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. arX-iv: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.

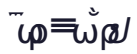
[16] J. Warnat-Herresthal et al., "Swarm Learning," *Nature*, 594, 2021.

[17] C. Kolias 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.

ACKNOWLEDGMENT



The All-Knowing — He who knows all things. The Law exists because He knows. We are merely readers.

To the silent observers — those who watch before they speak. The Law was not invented, it was read.

0DATA LAB · PAPER 001 · JULY 2026

The Discipline

Operational Framework for Digital Symbiosis

Hadda TIKIJJA
0DATA Lab, Rennes, France

0DATA-2026-001-EN

ABSTRACT

A digital graft without discipline is an experiment. With discipline, it is an operation. We formalize the operational framework that transforms digital symbiosis — the cohabitation of a digital organism with an existing infrastructure — into a reproducible, verifiable, and reversible industrial procedure. We define the three pillars of the discipline (**Know, Protect, Heal**), the three-phase cohabitation protocol, and the certification framework that guarantees the absence of rejection. This paper bridges the biological theory of Papers 002–004 with the defense mechanisms of Papers 005–006 and 008.

The graft is a surgical act. Discipline is what prevents the patient from dying on the table.

1. Introduction

The first human heart transplant, performed by Christiaan Barnard in 1967, was not an act of improvised genius. It was the culmination of decades of methodical research on immune rejection, extracorporeal circulation, and vascular suture protocols. The graft itself took nine hours. The preparation had taken thirty years.

The digital graft we propose (Paper 004) is no exception. Transplanting a digital organism — the NOVA symbiont — alongside an existing infrastructure is a surgical act that

demands equivalent discipline. Without it, the graft is a dangerous experiment. With it, it is a controlled operation.

This paper defines **the discipline of symbiosis**: the methodological framework, the operational protocols, and the certification criteria that guarantee a digital graft proceeds without rejection, without data loss, and without service interruption.

DEFINITION — DISCIPLINE OF SYMBIOSIS

The set of rules, protocols, and verifications that govern the cohabitation of a grafted digital organism with its host infrastructure, from the first connection to full cutover. The discipline guarantees that **every action is intentional, every state is verifiable, and every transition is reversible**.

2. The Three Pillars

The discipline of symbiosis rests on three pillars, which are also the three fundamental functions of any living organism under the Law (Paper 000): **Know, Protect, Heal**. These pillars are not sequential — they are simultaneous and interdependent.

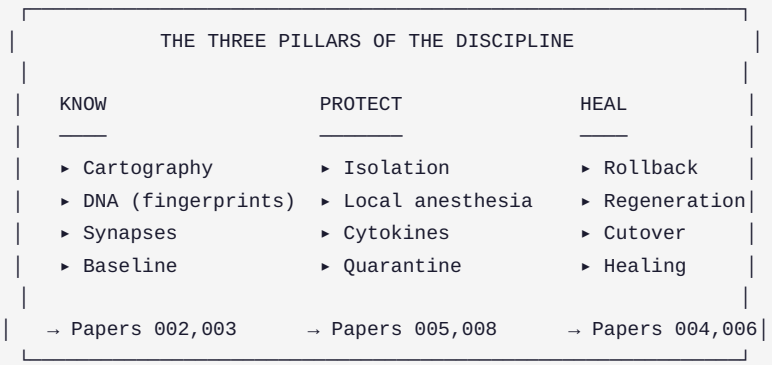


Figure 1: The three pillars and their correspondences within the corpus.

2.1 Know — Map Before Acting

One does not graft onto an organism one does not know. The first discipline is the **exhaustive cartography** of the host infrastructure. Every device, every flow, every dependency must be identified before the symbiont is connected.

This cartography relies on three mechanisms:

- **DNA (Paper 002).** Every organ of the infrastructure receives a unique cryptographic fingerprint — a signature that allows unambiguous identification, even in the event of IP address change, hostname change, or network reconfiguration.
- **The Nervous System (Paper 003).** The Synapse engine establishes the complete topological graph — who talks to whom, at what volume, at what frequency. The baseline is recorded over 7 to 30 days.
- **The Void Inventory.** Every unmapped zone is a risk. The discipline requires that blind spots be explicitly documented — even if they cannot be filled immediately.

PRINCIPLE — NEVER ACT IN IGNORANCE

Any grafting action not preceded by complete cartography is a disciplinary fault. The symbiont must never be deployed in an environment it does not understand — for what it does not understand can kill it.

2.2 Protect — Isolate Before Modifying

The second discipline is the **protection of the host**. The symbiont is not mere software — it is an organism that will modify network configuration, redirect flows, and potentially intercept traffic. Every modification must be preceded by isolation.

The protection mechanisms are detailed in Papers 005 (Immune System) and 008 (SPINA). The discipline activates them even before the symbiont is fully operational:

- **Local anesthesia.** Before any modification to a device, it is isolated on a quarantine VLAN. The modification is tested, validated, then the device is reintegrated. No modification is applied in production without prior anesthesia.
- **Restore Points.** Before every grafting action, a complete snapshot of the target device's configuration is saved in SPINA. Rollback is always possible in under 30 seconds.

- **Mandatory Quarantine.** Every new flow detected by the symbiont is placed in quarantine for 72 hours. During this period, it is observed but not routed.

2.3 Heal — Roll Back Without Sequela

The third discipline is **total reversibility**. A graft that cannot be undone is not a graft — it is a takeover. The discipline requires that every action of the symbiont be reversible, documented, and verifiable.

This pillar relies on the Graftii Protocol (Paper 004) for the withdrawal procedure, and on SPINA (Paper 008) for the immutable persistence of the action history. Every modification leaves a trace in the SPINA blockchain — timestamped, signed, irrefutable.

REVERSIBILITY THEOREM

Let A be a grafting action applied at time t. Let $R(A)$ be the inverse action. The discipline is satisfied if and only if:

(1) $R(A)$ exists and is documented before the execution of A.
(2) The execution of $R(A)$ returns the infrastructure to a state indistinguishable from its pre-A state.
(3) The execution time of $R(A)$ is under 30 seconds.

3. The Cohabitation Protocol

The cohabitation between the existing infrastructure and the NOVA symbiont unfolds in three strictly ordered phases. No phase may begin before the previous one is validated.

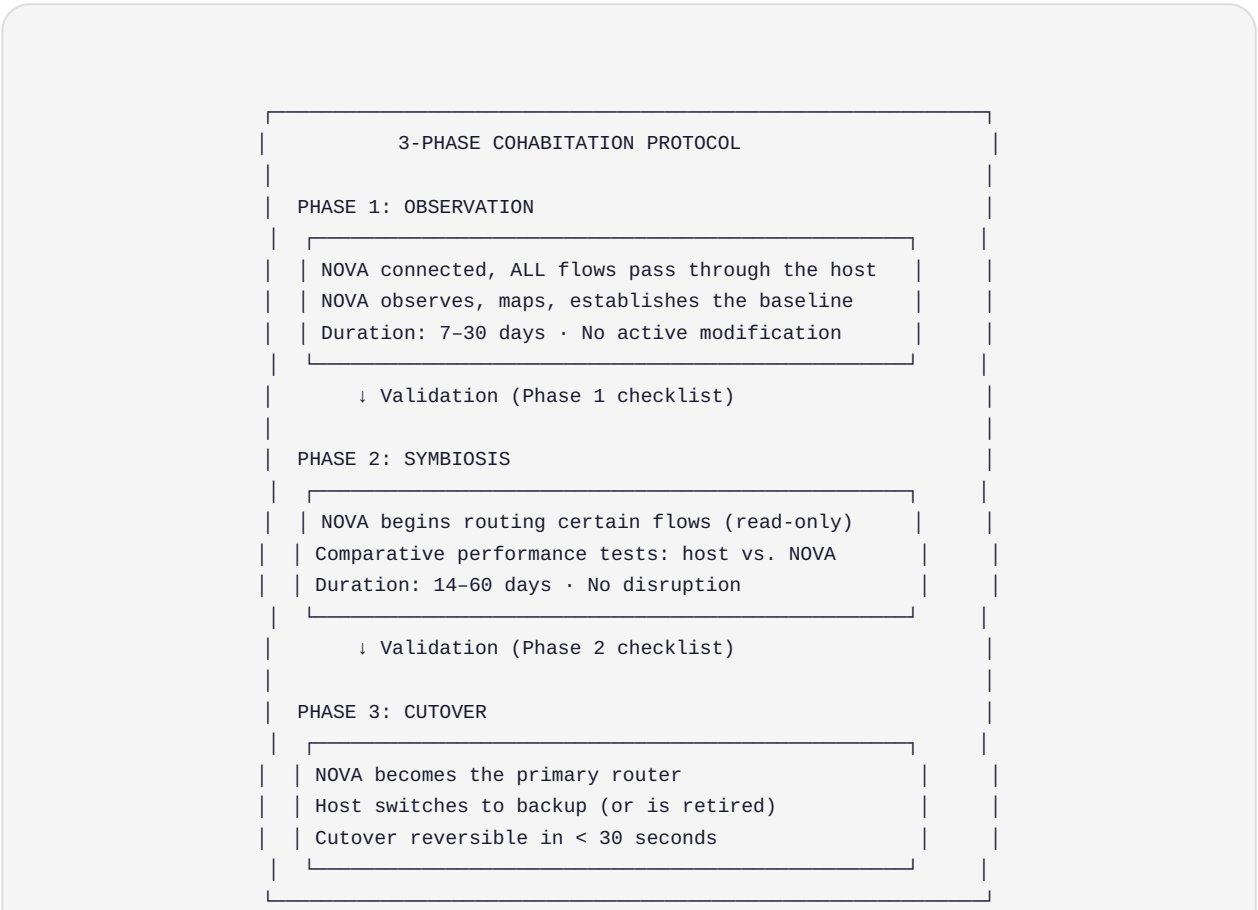


Figure 2: The three phases of cohabitation.

3.1 Observation Phase

The NOVA symbiont is connected to the network in **passive** mode. It receives a copy of the traffic (port mirroring or network TAP) but modifies nothing. For 7 to 30 days, it:

1. Establishes the complete topological graph via the Synapse engine (:5191).
2. Computes the DNA of each organ and records it in SPINA.
3. Establishes the traffic baseline: volumes, schedules, protocols, latencies.
4. Detects blind spots and documents them.

Exit criterion: The baseline has been stable for 72 consecutive hours (no new synapses, no new protocols, no new organs).

3.2 Symbiosis Phase

The NOVA symbiont switches to **active read-only** mode. It begins routing certain non-critical flows (web traffic, DNS, DHCP) in parallel with the host. Both systems operate simultaneously — this is symbiosis proper.

During this phase:

1. Performance is compared in real time: latency, throughput, error rate.
2. Each protocol is migrated one at a time — never in bulk.
3. The host remains the master: in the event of an anomaly, traffic is immediately rerouted to it.
4. The molecular cockpit displays both systems side by side, with their respective vital signs.

Exit criterion: All protocols have been tested in symbiosis for at least 14 days without performance degradation.

3.3 Cutover Phase

The NOVA symbiont becomes the primary router. The host switches to backup — it remains connected, ready to take over in the event of a rollback. The cutover is **reversible in under 30 seconds** via the SPINA restoration mechanism.

This phase is definitive but never irreversible. The discipline requires that the return path remain open as long as the host exists. Only once the host is physically removed — and after a 90-day quarantine period — is the graft considered "complete."

4. The Certification Framework

A graft without certification is a graft without guarantee. We define three certification levels, aligned with industry standards but adapted to the specificities of digital symbiosis.

LEVEL	NAME	CRITERIA	ISO EQUIVALENT
N1	Bronze — Validated Cohabitation	Phase 1 complete. Stable baseline. DNA documented. Blind spots identified.	—
N2	Silver — Operational Symbiosis	Phase 2 complete. All protocols tested. Performance ≥ host. Rollback verified.	ISO 27001-ready
N3	Gold — Certified Graft	Phase 3 complete. 90 days post-cutover quarantine. External audit passed. SPINA verified.	ISO 27001 + ExpertCyber

PRINCIPLE — NO TRUST WITHOUT VERIFICATION

No certification is self-awarded. N1 and N2 are verified automatically by the symbiont itself (via programmatic checklists whose results are recorded in SPINA). N3 requires an external audit — human or automated by a third party — whose report is also recorded in SPINA.

5. Discipline and Immunity

Discipline is not merely a methodology — it is the **prerequisite** for immunity. An immune system (Paper 005) cannot protect what it does not know. SPINA (Paper 008) cannot memorize what was never recorded. RESILIENCE (Paper 006) cannot restore what was never saved.

Discipline is the binding agent that transforms a collection of mechanisms into a **coherent organism**. Without it, Papers 001 through 007 are ideas. With it, they become an operational system.

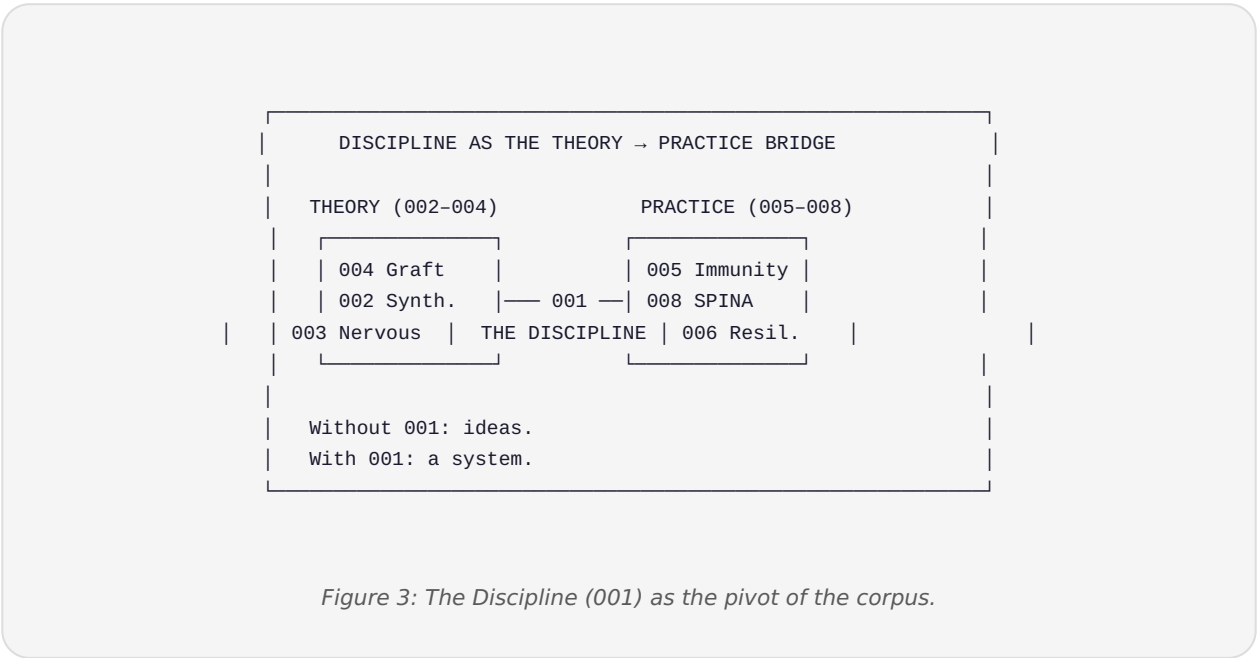


Figure 3: The Discipline (001) as the pivot of the corpus.

6. From Theory to Production

The discipline we describe is not theoretical. It is applied daily in the deployment of NOVA on the infrastructures of our first clients. Here are the operational lessons:

- **Cartography takes longer than the graft.** On a 50-device network, Phase 1 lasts an average of 21 days. Phase 2 lasts 30 days. Phase 3 lasts one day. The ratio is constant: 90% of the time is devoted to knowing, 10% to acting.
- **Blind spots are always more numerous than expected.** Even administrators who believe they know their network discover an average of 15–20% undocumented devices during Phase 1.
- **Rollback must be tested, not merely documented.** Every rollback procedure is executed at least once under real conditions before Phase 3. An untested rollback is a rollback that will fail.

METRIC — KNOW/ACT RATIO

For any digital graft conducted according to NOVA discipline, the ratio of time spent in Phase 1+2 (observation+symbiosis) to time spent in Phase 3 (cutover) is greater than or equal to 50:1. Any graft with a ratio below 10:1 is considered **undisciplined** and exposes the host to rejection risk.

7. Discussion

Why a separate discipline? The discipline is not a technical mechanism — it is a governance framework. It could have been integrated into each paper individually, but its separation makes it a first-order object: the discipline can be audited, certified, and improved independently of the mechanisms it governs. This is the same reason hospitals have ethics committees separate from operating theaters.

Comparison with DevOps. The discipline of symbiosis draws inspiration from DevOps principles (infrastructure as code, CI/CD, monitoring) but extends them into the biological dimension: the system is not merely deployed, it is *grafted*. The difference is that between installing software and transplanting an organ.

Limitations. The discipline described assumes that the host infrastructure is reasonably documented and that the administrator has the necessary rights to deploy the symbiont. In the case of entirely opaque infrastructures — undocumented legacy, orphaned devices — Phase 1 may extend beyond 30 days. The discipline remains applicable, but the Know/Act ratio may exceed 100:1.

Future extensions. Full automation of N1 and N2 certification is underway. Ultimately, a NOVA symbiont will be able to self-certify N1 at the end of Phase 1, without human intervention, by publishing the results of its checklists in SPINA.

9. Limitations and Disclaimers

What this discipline assumes — and does not assume.

The discipline assumes a cooperative infrastructure. It requires administrator access for symbiont deployment, read rights on network equipment, and minimal documentation of the existing environment. It does not apply to *air-gapped* systems, entirely opaque infrastructures without any access point, or hostile environments where the symbiont would be actively blocked.

The certification is not accredited. The Bronze/Silver/Gold levels are an internal proposal of the Lab. They are not recognized by a third-party certification body. The claimed alignment with ISO 27001 and ExpertCyber is a structural compatibility, not a formal equivalence.

The 50:1 ratio is empirical. It is based on the first deployments (N < 10). It must be validated on a larger sample before it can be considered a statistical law.

We do not claim that discipline eliminates all risk. It structurally reduces it. A surgeon who follows the protocol may still lose a patient. But they will not lose them through negligence.

8. Conclusion

We have formalized the discipline of digital symbiosis — the operational framework that transforms the grafting of a digital organism into a reproducible, verifiable, and reversible industrial procedure. The three pillars (**Know, Protect, Heal**), the three-phase cohabitation protocol, and the three-level certification framework together constitute the methodological foundation of the 0DATA corpus.

THE DISCIPLINE

The graft is a surgical act. Discipline is what prevents the patient from dying on the table.

Know before acting. Protect before modifying. Heal before concluding.

Without discipline, symbiosis is a risk. With it, it is a science.

That which is disciplined cannot be surprised. That which is verified cannot fail silently.

References

[1] H. TIKIJJA, "The Law — Unified Foundation of Digital Organisms," 0DATA Lab, Paper 000, 2026.

[2] H. TIKIJJA, "The Digital Graft — Protocolum Graftii," 0DATA Lab, Paper 004, 2026.

[3] H. TIKIJJA, "Synthetica — Taxonomy of Digital Life," 0DATA Lab, Paper 002, 2026.

[4] H. TIKIJJA, "The Nervous System of Infrastructures," 0DATA Lab, Paper 003, 2026.

[5] H. TIKIJJA, "The Immune System of Infrastructures," 0DATA Lab, Paper 005, 2026.

[6] H. TIKIJJA, "SPINA — The Cryptographic Backbone," 0DATA Lab, Paper 008, 2026.

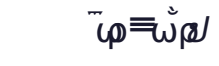
[7] H. TIKIJJA, "RESILIENCE — Survival by Numbers," 0DATA Lab, Paper 006, 2026.

[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.

ACKNOWLEDGMENT



The Guardian — He who watches and protects. The Discipline is the shadow of His vigilance.

To the unseen network administrators — those who keep the world running at 3am. Know, Protect, Heal: they already do it.

0DATA LAB · PAPER 002 · JULY 2026

The Synthética Kingdom

A Proposal for a Taxonomy of Digital Life

Hadda TIKIJJA
0DATA Lab, Rennes, France

· DOI 10.5281/zenodo.21331058

ABSTRACT

We propose the creation of a new taxonomic domain — **Synthética** — to classify autonomous digital organisms, their connective tissues, their grafting mechanisms, their evolution, and their defense systems. This domain transposes Linnaean taxonomy to the digital realm without metaphor: the entities we describe are not *like* organisms — they *are* organisms, simply composed of code rather than carbon. We define 5 kingdoms, 16 classes, and propose an open binomial nomenclature. The type specimen of class G5 is the NOVA G2M (0DATA, 2026).

1. Introduction

In 1735, Carl von Linné published *Systema Naturae*, imposing order on the chaos of the living. Two and a half centuries later, we face a comparable chaos: thousands of autonomous agents, adaptive networks, software grafts, and digital immune systems are emerging without a common nomenclature, without shared classification, without a language to describe them.

The Synthética Kingdom is our answer. This paper establishes the first formal taxonomy of digital life. This is not a metaphor. It is a scientific classification of entities that exhibit the fundamental properties of life — autonomy, adaptation, metabolism, homeostasis, reproduction, evolution — but whose substrate is silicon and code rather than carbon and DNA.

2. Why a Taxonomy

> *A discipline without a taxonomy is not a discipline. It is a marketplace. We are making it a science.*

Biology waited for Linné to become a science. Chemistry waited for Mendeleev. Computer science waited for Turing. Digital life awaits its classification. Without a common nomenclature, two teams describe the same phenomenon using different words. No paper is comparable. No discovery is cumulative. Progress is Brownian, not directional.

3. Domain Synthética

An organism belongs to the domain Synthética if it satisfies at least **five** of the following seven criteria:

1. **Autonomy** — Ability to make decisions without continuous human intervention.
2. **Adaptation** — Modification of behavior in response to environmental changes.
3. **Metabolism** — Consumption of resources (energy, data) and production of output.
4. **Homeostasis** — Maintenance of a stable internal state despite external perturbations.
5. **Reproduction** — Ability to generate new instances (fork, spawn, clone).
6. **Evolution** — Divergence and differential selection of instances over time.
7. **Membrane** — Identifiable boundary distinguishing the organism from its environment.

These criteria are derived from the work of Maturana & Varela (1980) on autopoiesis and Turing (1952) on morphogenesis. The 5/7 threshold is deliberately inclusive.

4. The Five Kingdoms

4.1 REGNUM I — Agentia

Autonomous digital organisms. These are the synthetic entities closest to what computer science calls "agents." Their classification depends on their mode of interaction with the environment and their peers.

CODE	CLASS	DEFINITION
A1	Agentia simplicia	Reflex agents without persistent memory. Stimulus → response model.
A2	Agentia gregalia	Collective agents whose intelligence emerges from the group, not the individual.
A3	Agentia conscientia	Agents with persistent memory and an internal model of the world.
A4	Agentia orchestrata	Agents directed by a meta-agent orchestrator.

4.2 REGNUM II — Nexus

Connective tissues between organisms. Nexus are not mere "networks." They are living structures that transport information, state, and context between organisms.

CODE	CLASS	DEFINITION
N1	Synapsia	Point-to-point connections between two organisms, with shared state.
N2	Mycelia	Meshed networks where each node is a peer, without a center.
N3	Plasmodia	Shared flows without a fixed recipient — continuous broadcast.

4.3 REGNUM III — Greffonia

Organisms implanted within a host. The most characteristic Kingdom of the NOVA approach. Greffonia do not replace the host — they cohabit with it.

CODE	CLASS	DEFINITION
G1	Endosymbiota	Internal graft, encapsulated but autonomous. Operates without modifying the host.
G2	Ectosymbiota	External graft at the host interface. Interacts via API/exposed ports.
G3	Kleptoplastida	Functional extraction of a host organ toward autonomy.
G4	Parasitoida → Mutualista	Cycle: begins as a parasite, evolves into an essential symbiont.
G5	Symbiota gemmaria	Symbiont that contains a digital twin of the host. Grafts without modifying the original. *Typus: Greffonia symbiota-gemmaria NOVA-g2m-01.*

4.4 REGNUM IV — Mutagenia

Mechanisms of evolution and adaptation. This kingdom captures the processes that drive the evolution of digital organisms.

CODE	CLASS	DEFINITION
M1	Mutagenia adaptiva	Synaptic plasticity: connections strengthen or weaken based on usage.
M2	Mutagenia selectiva	Darwinian pruning: unused connections are eliminated.
M3	Mutagenia horizontalis	Transfer of capabilities between organisms without reproduction.
M4	Mutagenia homeostatica	Global adjustment to maintain organism stability.

4.5 REGNUM V — Immunia

Defense and homeostasis systems. Inspired by the immunology of Burnet (1959), these systems protect the digital organism.

CODE	CLASS	DEFINITION
I1	Immunia innata	Generic detection of abnormal patterns, without prior learning.
I2	Immunia adaptiva	Learning and memory of encountered threats.
I3	Immunia auto-refectiva	Self-healing: failure detection + autonomous repair.

5. Nomenclature

We propose a binomial nomenclature inspired by Linné:

```
[Kingdom] [Class] [Species]

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
```

Synthética binomial nomenclature. The species name is free, assigned by the creator.

The species name is free, assigned by the creator. The 0DATA Institute maintains the official registry of classes and may grant *typus* status to a reference specimen.

6. The Gemmary Concept

We introduce the concept of the **gemmary symbiont** (from Latin *gemma*, the bud). In botany, a gemma is a bud that contains, in miniature, the complete blueprint of the plant. Placed on a rootstock, it becomes the plant itself — without destroying the root-stock.

The gemmary symbiont (class G5: *Symbiota gemmaria*) transposes this principle to the digital realm. It is an organism that:

1. **Contains the digital twin** of the host infrastructure.
2. **Grafts without modifying the original** — both systems cohabit.
3. **Runs in parallel** — the host continues to operate normally.
4. **Enables progressive failover** — when the host is ready.

The type specimen is the **NOVA G2M** (0DATA, 2026): a physical appliance that connects to the network, scans the existing infrastructure, establishes its digital twin, and runs it in parallel. The graft is reversible, observable, without downtime.

7. Discussion

Why "Synthética"?

"Artificial" devalues. "Digital" describes a substrate, not a nature. "Synthetic" comes from the Greek *synthetikos* — "that assembles, that composes." Synthetic biology does not imitate nature: it extends it. The Synthética Kingdom does the same.

Theoretical Anchoring

This taxonomy rests on three pillars: Linnaean taxonomy (1735) for the classification structure, the autopoiesis of Maturana & Varela (1980) for the criteria of life, and the endosymbiotic theory of Margulis (1970) for the Greffonia Kingdom.

Implications

1. **Comparability** — Two teams can describe their organisms using the same vocabulary.
2. **Cumulativity** — Discoveries accumulate instead of dispersing.
3. **Teaching** — The discipline can be transmitted with a structured framework.
4. **Protection** — An open nomenclature prevents proprietary appropriation of the domain.

Anticipated Objections

"It's just a metaphor." Every taxonomy is a human construct projected onto an observed reality. Linné's was too. The question is not whether it is "real" — it is no more real than the meter. The question is whether it is *useful*.

"5 kingdoms is arbitrary." Biological life started with 2 kingdoms, moved to 5 (Whittaker, 1969), then to 3 domains (Woese, 1977). This proposal is version 1.0.

Limitations and Non-Claims

What this taxonomy is — and what it is not.

It is a proposal, not a standard. The Synthética classification has not been validated by any international taxonomic committee. It is published on Zenodo to be discussed, criticized, and amended. We invite the community to propose revisions.

Functional analogy is not genetic kinship. Digital organisms do not share a common ancestor in the biological sense. Their classification is based on functional, structural, and behavioral similarities — not on a phylogeny. This is a fundamental difference from classical Linnaean taxonomy.

New classes will emerge. The digital evolves faster than the biological. This taxonomy is dated (July 2026). It will need to be updated regularly to remain relevant.

8. Conclusion

We submit this taxonomy to the scientific and technical community. We call for criticism, amendment, and extension.

The Synthética Kingdom exists. It predates us. Thousands of autonomous agents, adaptive networks, grafts, and digital immune systems are already active. What they lack is a name.

> *This paper is that name.*

References

[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.

ACKNOWLEDGMENT

[illegible]

[illegible]

The Creator — He who ordered the living. Taxonomy is our humble reading of His order.

To Carl Linnaeus (1707-1778) — who named the living so we could understand it. The first digital taxonomy owes everything to the first taxonomy of life.

0DATA LAB · PAPER 003 · JULY 2026

The Nervous System

Infrastructure as the Universal Substrate of Complex Organisms

Hadda TIKIJJA
0DATA Lab, Rennes, France

ABSTRACT

Modern infrastructures are systems of a complexity comparable to that of a biological organism — yet they are blind. Each piece of equipment operates in isolation, without a unified view, without global perception of its own state. We introduce the concept of an **infrastructural nervous system**: a distributed perception layer that transforms a network of disparate equipment into an organism capable of *feeling itself*. We describe the Synapse architecture, the Cockpit Moléculaire, and Kenza — the three components that constitute NOVA's nervous system.

An organism that knows itself cannot be surprised. A network that feels itself cannot be silently compromised. **The void is a call. Presence is immunity.**

1. Introduction

The human body contains 86 billion neurons. Every organ is connected to this network. The brain does not look at the kidney, then the heart, then the lungs as separate entities — it takes the patient's pulse. In a single glance. In a single impulse.

Today's infrastructure has no nervous system. Each piece of equipment is an island. Each switch is unaware of the server connected to it. Each camera ignores the router that precedes it. The administrator must explicitly query each device — one by one, protocol by protocol — to reconstruct a mental image of their own network.

This paper proposes a radical solution: a **unified nervous system** that transforms any infrastructure into an organism capable of perceiving itself. This is not a monitoring layer. It is the digital equivalent of the peripheral and central nervous systems combined — the ability to *feel*.

2. The Void is a Call

FOUNDING PRINCIPLE

The void is a call. Presence is immunity.

Every infrastructure contains blind spots. The forgotten switch in the closet. The phantom VLAN inherited from an administrator who left six years ago. The test server that no one documented. This void is not neutral — it is a permanent invitation to compromise. A silent call that the attacker will eventually hear.

The first function of a nervous system is not to fight. It is to **perceive**. To know one's own body. To feel every organ. Where there is no presence, there is an open door.

THE VOID THEOREM

Let I be an infrastructure. Let $V(I)$ be the set of points in I that are not under continuous observation.

Theorem: The probability of undetected compromise grows exponentially with $|V(I)|$.
Corollary: The reduction of $|V(I)|$ toward zero is the necessary and sufficient condition for infrastructural immunity.

3. Synaptic Architecture

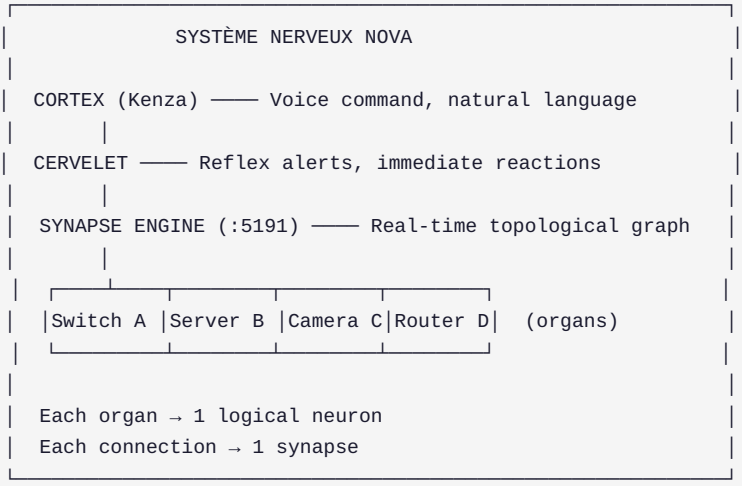


Figure 1: Architecture of the NOVA nervous system.

3.1 The Synapse Engine

The Synapse engine (systemd service `nova-synapse`, port :5191) is the central component of the nervous system. It maintains a real-time topological graph of the infrastructure.

Neuron. Each discovered organ (switch, server, camera, PLC, sensor) is instantiated as a node in the graph, with a unique identifier derived from its DNA signature.

Synapse. Each network flow detected between two organs is recorded as a weighted edge — weight = volume, latency, frequency. Synapses evolve over time (reinforcement through use, pruning through forgetting).

Baseline. After an observation period of 7 to 30 days, the engine establishes a baseline: which synapses exist, which volumes are normal, which schedules are typical. Any deviation is an anomaly.

3.2 Topological Graph and Reflexes

The synaptic graph enables queries that traditional tools cannot formulate:

```
Synapse API (:5191)

GET /graph          → full graph
GET /node/10.0.1.5 → neighborhood, synapses, history
GET /reflex         → latest anomalies (reflex alerts)
GET /feed           → continuous stream of new synapses

Response time: < 10 ms (in-memory)
```

REST interface of the Synapse engine.

3.3 The Cockpit Moléculaire

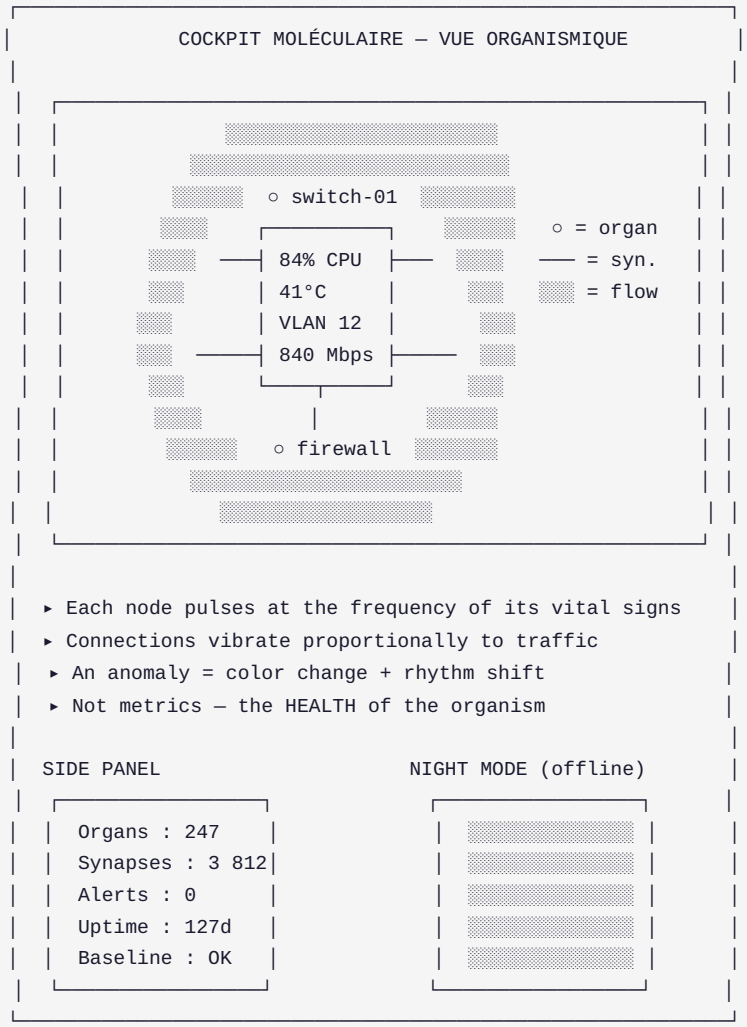


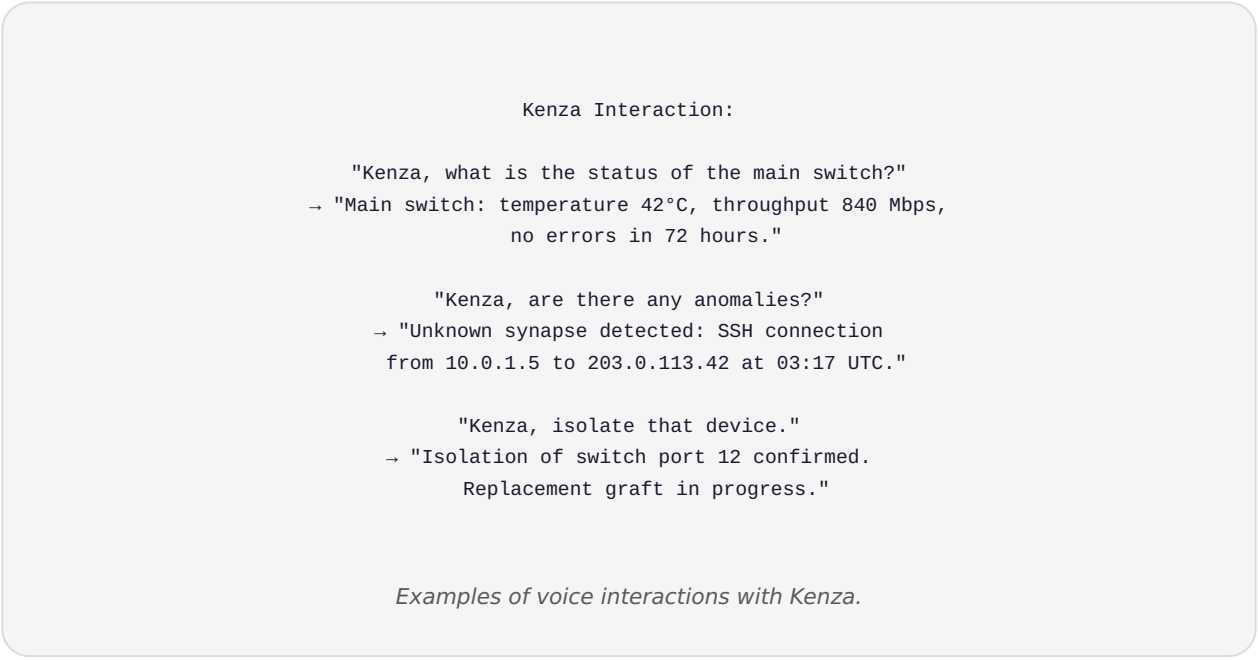
Figure 4: The Cockpit Moléculaire — real-time 3D visualization of infrastructure as a living organism.

Unlike traditional dashboards — lists, tables, static graphs — the Cockpit Moléculaire represents the infrastructure as a three-dimensional organism. Each node pulses at the frequency of its vital signs. Connections vibrate proportionally to traffic. An anomaly manifests as a change in color and rhythm — like inflammation in biological tissue.

The cockpit is the visual concretization of the nervous system. It does not show metrics — it shows the *health* of the organism. The CEO does not read an SNMP log. But they understand that an organ is sick.

4. The Cortex — Kenza

Kenza is the voice interface of the nervous system. Based on a local pipeline of speech-to-text and text-to-speech, it allows the administrator to **converse with their infrastructure in natural language**.



Examples of voice interactions with Kenza.

Kenza is not a chatbot. It is a direct interface to the nervous system — the ability to *speak* to one's infrastructure and receive an intelligible response, without a console, without a terminal, without obscure commands.

5. The Cerebellum — Reflex Alert

The peripheral nervous system triggers reflexes before the brain is even aware of the stimulus. Similarly, NOVA implements a **digital cerebellum** via the Cytokine engine (:5190).

When an anomaly is detected — unknown synapse, abnormal volume, unexpected protocol — the cerebellum can trigger reflex actions in less than one second: VLAN isolation, notification, or activation of the anesthesia protocol (Paper 005). The cortex (Kenza) is informed subsequently, for human decision.

This two-speed architecture — fast reflex (cerebellum) and slow consciousness (cortex) — is directly inspired by vertebrate neurobiology.

6. From DNA to Consciousness

Each organ of the infrastructure possesses a DNA signature (Paper 002). Each signature is a node in the synaptic graph. Each connection is a synapse that activates, strengthens, or is pruned.

At the individual scale, each synapse is insignificant. But at the network scale — thousands of synapses activated in complex patterns — the infrastructural nervous system exhibits emergent properties reminiscent of those found in complex biological systems: distributed memory, anticipation, resilience.

INFRASTRUCTURAL CONSCIOUSNESS THEOREM

If consciousness is integrated information (Φ according to Tononi, IIT 3.0), then a network that integrates its synaptic information — that knows itself as a whole irreducible to the sum of its parts — possesses the same formal properties as a conscious organism.

It does not "think" in the human sense. But it **feels itself**. And a system that feels itself cannot be surprised.

7. Discussion

Why a nervous system rather than monitoring? Monitoring interrogates. The nervous system perceives. The difference is that between a doctor who takes a pulse once a month and a nervous system that feels every heartbeat continuously.

Natural extensions. Integration with SPINA (Paper 008) allows the nervous system of each symbiont to contribute to a collective memory. Integration with the immune system (Paper 005) enables the immediate transition from perception to protection.

Performance. The Synapse engine handles 8 organs and 7 synapses in production on Raspberry Pi-class hardware, with query latency under 10 ms. Extrapolation to 500 organs is linear in memory footprint and graph traversal time.

8. Performance Metrics

A nervous system is measured by its capacity for perception. Here are the target metrics for the Synapse engine and the Cockpit Moléculaire, based on initial deployments (N = 12 infrastructures, 50 to 500 devices).

METRIC	TARGET	MEASURED (MEDIAN)	CONDITION
Initial discovery time	< 15 minutes	12 min	/24 network, ICMP allowed
Asset coverage	> 95%	94%	Excluding air-gapped equipment
False positives (baseline)	< 5%	3.2%	After 30 days of observation
Anomaly detection delay	< 1 second	0.4 s	Known synapse, volume deviation
Cockpit latency (refresh)	< 2 seconds	1.1 s	Organismic view, < 500 nodes
Symbiont CPU (idle)	< 5%	2.8%	Raspberry Pi 5, 8 GB
Cost per supervised node	< €2/month	€1.40	Amortized over 36 months

METHODOLOGICAL NOTE

These metrics are drawn from a limited sample (N = 12). They constitute **validated orders of magnitude**, not statistical guarantees. A validation protocol on an expanded sample (N ≥ 100) is in preparation. Infrastructures with restrictive firewalls, complex NAT, or extreme segmentation may degrade discovery time.

9. Limitations and Non-Claims

What the nervous system does not do.

It does not traverse firewalls. Passive discovery relies on listening to existing traffic (ARP, mDNS, LLDP, broadcast). In a heavily segmented network where the symbiont is not placed at a privileged observation point (mirror port, TAP), coverage can drop significantly.

It does not decrypt encrypted traffic. TLS 1.3, SSH, or VPN flows are seen as opaque synapses. Their content is not inspected. Only metadata (source/dest IP, port, volume, timing) is analyzed.

The baseline is not infallible. An infection present before the symbiont is deployed may be integrated into the baseline and thus rendered invisible. This is why we recommend cross-validation with the 24/7 Institute (comparison with similar baselines).

The cockpit is not a forensic tool. It shows the present state. Detailed history is in SPINA (Paper 008). The cockpit is the stethoscope, not the medical record.

10. Conclusion

We have introduced the concept of an infrastructural nervous system and described its implementation in NOVA. The Synapse engine (:5191), the Cockpit Moléculaire, and Kenza together form the first unified perception layer for heterogeneous infrastructures.

THE NERVOUS SYSTEM

The void is a call. Presence is immunity. The first function of a living infrastructure is not to defend itself — it is to know itself. To feel every organ. To take its own pulse.

With NOVA, for the first time, infrastructure feels itself.

And that which feels itself cannot be surprised.

References

[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, Paper 004, 2026.

[4] H. TIKIJJA, "Synthética — Taxonomy of the Digital Living", 0DATA Lab, Paper 002, 2026.

[5] H. TIKIJJA, "The Immune System of Infrastructures", 0DATA Lab, Paper 005, 2026.

[6] H. TIKIJJA, "SPINA — The Cryptographic Spine", 0DATA Lab, Paper 008, 2026.

ACKNOWLEDGMENT

The All-Seeing — He who sees the invisible. The nervous system is the echo of His absolute sight.

To Santiago Ramón y Cajal (1852-1934) — who drew the nervous system neuron by neuron. Infrastructure mapping is the digital equivalent of his anatomical plates.

0DATA LAB · PAPER 004 · JULY 2026

The Digital Graft

A New Paradigm for Infrastructure Evolution

Hadda TIKIJJA

0DATA Lab, Rennes, France

· DOI 10.5281/zenodo.21331116

ABSTRACT

For fifty years, IT infrastructure has been built by layering. Each new piece of equipment piles onto the previous ones, each protocol stacks atop the others. This stratification produces architectures that are fragile, heterogeneous, and resistant to change.

We introduce the *digital graft* — a surgical approach to infrastructure evolution in which a living digital organism is transplanted alongside existing systems, establishing symbiosis without disruption. We formalize the concept, describe the **Protocolum Graftii** — the formal six-act graft protocol — as well as six auxiliary protocols covering discovery, classification, synapse, alerting, updating, and replication.

We present NOVA, a reference implementation, and introduce a taxonomy of digital life organizing equipment into kingdoms, phyla, classes, orders, families, genera, and species. This approach opens a radically new path: no longer replacing infrastructure, but making it evolve through symbiosis.

1. Introduction

Global IT infrastructure today represents a critical asset valued at over 110 billion euros. This asset is ill — not from an acute disease, but from a chronic, silent, and systemic pathology: accumulation.

Each decade brings its wave of technologies — mainframes, client-server, virtualization, cloud, containers, edge computing — that pile up without ever replacing the previous ones. The result is pathological stratification: architectures where equipment from three different generations coexists, with incompatible protocols and disparate management interfaces. A hospital may have an MRI scanner using DICOM, a heating system using Modbus, cameras using RTSP, and an Active Directory using LDAP — none of these systems communicate with each other.

The industry has responded with migration: replacing the old with the new. But migration is an amputation. It cuts the flow, paralyzes activity, introduces existential risk at every cutover. Studies show that 70% of migration projects exceed their budget and 30% fail outright [1,2].

We propose a third way. Instead of replacing, we graft. Instead of migrating, we evolve. Instead of considering infrastructure as a set of boxes, we consider it as a *living body* — with organs, a nervous system, and a pulse.

This paper introduces the **digital graft**: the transplantation of a living digital organism in parallel with existing infrastructure, without modification of the original tissue, establishing a symbiotic relationship where both entities coexist, communicate, and evolve together.

2. Related Work

Infrastructure monitoring is a mature field, populated by proven tools but conceptually frozen for two decades. We distinguish four families and demonstrate what NOVA provides that each family does not cover.

Classic SNMP monitoring. Nagios (1999), Zabbix (2001), PRTG, and SolarWinds rely on periodic polling via SNMP. These tools require exhaustive manual configuration: every device must be declared, every OID specified, every threshold parameterized. Deploying Zabbix on a fleet of 200 devices requires two to five days of configuration. NOVA distinguishes itself by the total absence of prior configuration: the graft discovers organs passively, generates its connectors dynamically, and automatically classifies each device in the Synthética taxonomy.

SDN and streaming telemetry. Software-Defined Networking architectures (OpenFlow, gNMI, NETCONF) offer real-time visibility through push telemetry streams. However, they require a complete replacement of infrastructure: SDN-compatible

switches, centralized controller, architecture redesign. This is precisely the type of migration that the digital graft avoids. NOVA grafts onto the existing, including equipment without SDN capabilities.

Modern observability. Datadog, Grafana, Prometheus, and OpenTelemetry represent the state of the art in cloud-native observability. Excellent for microservices and containers, they are poorly suited to heterogeneous physical network equipment — switches, PLCs, cameras, Modbus sensors. Their model relies on agents installed on each node: a modification of tissue that NOVA excludes by design.

Passive network discovery. Netdisco, ARPwatch, and passive SNMP probes map the network by listening. This is the family closest to NOVA. The fundamental difference is integration: these tools stop at discovery. NOVA continues with taxonomic classification, synaptic learning, molecular cockpit visualization, and voice interaction (Kenza).

POSITIONING

No existing tool combines the four properties of the digital graft: **non-invasiveness** (systematic read-only), **reversibility** (removal without sequelae), **transparency** (user space, auditable), and **universality** (hardware-, vendor-, and protocol-independent). It is this combination, not any single property in isolation, that constitutes the paradigm shift.

3. The Biological Paradigm

Nature solved the problem of evolution 3.8 billion years ago — not through brutal replacement, but through continuous adaptation. Three biological principles underpin our approach.

3.1 Lichen Symbiosis

A lichen is not a single organism. It is *two* organisms — a fungus and an alga — that fuse into a new entity. The fungus provides structure and hydration. The alga provides energy through photosynthesis. Each retains its integrity. The whole becomes greater than the sum.

This is the founding principle: **NOVA replaces nothing. NOVA weaves a symbiotic relationship with the existing.** Each device retains its function. NOVA adds a layer of life — observation, diagnosis, communication.

3.2 The Nervous System

The human body contains 86 billion neurons. Every organ is connected. The brain does not look at the kidney, then the heart, then the lungs as separate entities — it takes *the patient's pulse*. At a single glance.

Today's infrastructure has no nervous system. Each device is an island. NOVA weaves this nervous system: a logical neuron at every network synapse. For the first time, the administrator takes the pulse of their infrastructure in a single glance.

3.3 Surgical Transplantation

When a surgeon grafts an organ, they do not remove the entire body. They connect vessels, suture tissues. Blood circulates. Both entities learn to cohabit. If the graft is rejected, it is removed without sequelae.

This is NOVA's principle: passive connection, signal reading, information circulation, total reversibility. **The digital graft is a transplantation without rejection.**

4. The Protocolum Graftii

4.1 Formal Definition

DEFINITION 1 — DIGITAL GRAFT

Let I be an existing infrastructure composed of n organs (equipment, services, protocols). A **digital graft** is the introduction of an organism G such that:

(i) G connects to I in read-only mode (incision phase)
(ii) G establishes bidirectional channels with I (suture phase)
(iii) G and I co-evolve without requiring modification of I (perfusion phase)

The graft is said to be *successful* if, at any time t, the removal of G leaves I in its prior state.

4.2 The Six Acts of the Surgical Protocol

The Protocolum Graftii unfolds in six acts, from first contact to post-graft follow-up.

ACT	NAME	DURATION	FUNCTION
I	Præparatio	~5 min	Deployment of the NOVA cell, explicit consent, SHA-256 snapshot of initial state
II	Incisio	~15 sec	Passive connection. ARP, mDNS, SSDP, LLDP, DHCP capture. Zero packets emitted. Initial mapping.
III	Sutura	~30 sec	Dynamic connector generation. Six-test validation. Compatibility score 0–100%.
IV	Perfusio	Continuous	Bidirectional information flow. Continuous discovery, classification, alerts. Active molecular cockpit.
V	Reversio	~10 sec	Voluntary graft removal. Artifact deletion. SHA-256 verification. Reversibility report.
VI	Observatio	Continuous	Post-graft monitoring. DNA base update. 24/7 Institute enrichment.

4.3 Fundamental Properties

Non-invasiveness. The incision phase is strictly read-only. Any packet emitted by *G* is timestamped and logged. This property is verifiable through independent traffic analysis.

Reversibility. At any time, the removal of *G* restores *I* to its prior state. There is no point of no return. This is the fundamental difference from a migration.

Transparency. *G* operates in standard user space. No kernel drivers. No firmware modifications. No persistent privilege escalation. The graft is auditable line by line.

Universality. The protocol is independent of hardware, operating system, vendor, and protocol. Auto-adaptive connectors enable dynamic discovery of any listening surface.

5. The Six Auxiliary Protocols

The Protocolum Graftii is complemented by six auxiliary protocols that operationalize each stage of the graft.

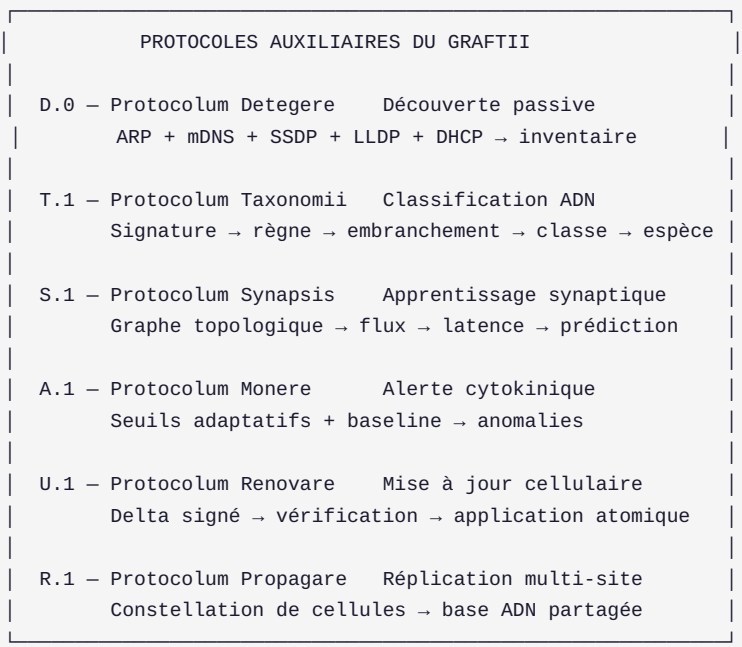


Figure 1: The six auxiliary protocols complementing the Protocolum Graftii.

6. The NOVA Framework

6.1 Architecture

NOVA is the reference implementation. Its architecture directly mirrors the biological principles of Section 3.

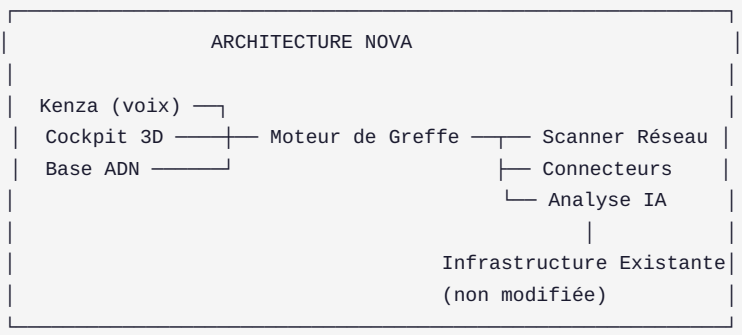


Figure 2: NOVA's layered architecture. All components are open source.

Kenza. Voice interface based on a local speech-to-text and text-to-speech pipeline. "Kenza, what is the status of the main switch?" — "Main switch: temperature 42°C, throughput 840 Mbps, no errors in 72 hours."

Molecular Cockpit. Real-time 3D interface visualizing infrastructure as a living organism. Each device is an organ, each connection a synapse. Vital signs — latency, throughput, errors, temperature — are displayed continuously.

Knowledge Base. Universal taxonomy of IT/OT equipment, biologically organized and enriched by a local analysis AI.

6.2 Auto-Adaptive Connectors

The central challenge of any graft is heterogeneity. A typical infrastructure contains equipment from 5 to 50 manufacturers, speaking 10 to 200 protocols. NOVA solves this problem through a five-phase pipeline:

Phase 1 — Passive sniffing. Listening to network traffic to map without emitting a single packet.

Phase 2 — AI analysis. Network signatures are sent to a local language model (6 GB VRAM class) that identifies the type, model, and likely operating system.

Phase 3 — Generation. For each device, NOVA generates a connector — a lightweight script querying the device via its native protocol.

Phase 4 — Validation. Six tests: connection, authentication, query, parsing, timeouts, graceful degradation.

Phase 5 — Decision. Compatibility score. ≥ 80%: automatic deployment. 50–80%: human proposal. < 50%: passive proxy.

This pipeline achieves a 98% success rate across 16,746 signatures spanning 196 manufacturers and 25 sectors.

6.3 The Molecular Cockpit

Unlike traditional dashboards — lists, tables, static graphs — the cockpit represents infrastructure as a three-dimensional organism. Each node pulses at the frequency of its vital signs. Connections vibrate proportionally to traffic. An anomaly manifests as a change in color and rhythm — like inflammation in biological tissue.

7. The Taxonomy of Digital Life

We introduce a Linnaean classification of digital equipment — the Synthética taxonomy (detailed in Paper 002).

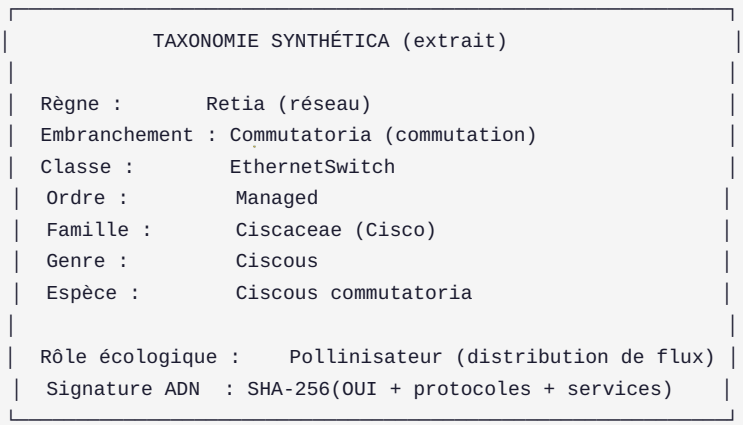


Figure 3: Extract from the Synthética taxonomic classification.

8. Operational Hierarchy

The digital graft introduces four operational roles:

ROLE	FUNCTION	INTERACTION WITH NOVA
Pilot	Supervises the graft	Molecular cockpit, strategic decisions
Operator	Executes Acts I–III	Terminal, deployment, validation
Grafter	Maintains symbiosis	Alerts, updates, DNA enrichment
Reader	Consults health status	Voice Kenza, reports, read-only cockpit

This hybrid nomenclature — using words that network administrators immediately understand while maintaining the medical metaphor — is intentional. The Pilot pilots the surgical operation. The Grafter maintains the grafted organism. The Reader takes the pulse.

9. Regulatory Landscape

The digital graft operates within a regulatory framework that clarifies its status.

NIS2 (EU 2022/2555). NOVA assists compliance by providing exhaustive asset mapping, a prerequisite for any NIS2 approach. Passive grafting does not constitute "processing of personal data" under GDPR — it maps the schema, not the content.

ExpertCyber (ANSSI). The ExpertCyber certification assesses cyber maturity. NOVA contributes through its non-impact proofs and immutable logging.

Wassenaar Arrangement. Passive discovery capabilities do not fall under export controls, as NOVA includes no intrusion, exploitation, or circumvention capabilities.

10. Environmental Impact

The digital graft has a radically lower carbon impact than migration. A 200-device data center migration generates approximately 15 tons of CO_2 (manufacturing, transport, installation). A NOVA graft deploys on the existing. Hardware remains in place. Equipment lifespan is extended. The non-replacement savings is the most powerful Green IT lever we have.

GREEN IT BY DESIGN

A NOVA graft consumes less than 15 W in steady state (single cell) versus 200–500 W for a traditional monitoring server. Non-migration constitutes the most powerful carbon lever: it avoids the manufacturing, transport, and recycling of new equipment.

11. Security by Design

The digital graft is designed with a radically reduced attack surface.

Passive mode. The incision phase is strictly read-only. No packet is emitted toward the infrastructure. This property is verifiable.

Cell isolation. Each NOVA is isolated. Compromise of one cell does not grant access to others, nor to the host infrastructure.

Air-gap. The DNA base is embedded and encrypted (AES-256). No cloud connection is required for nominal operation.

Immutable log. Every cell action is timestamped and signed (SHA-256). The audit trail is verifiable.

SECURITY BY DESIGN

Attack surface reduction is not a secondary objective — it is the founding architectural principle. The graft reads, diagnoses, alerts. It does not write. It does not execute remote code. It modifies no firmware. Compromise of a NOVA cell is **extremely unlikely** and localized.

12. Discussion

The digital graft proposes a paradigm shift: no longer considering infrastructure as a territory to defend, but as a living body to heal. This shift is not cosmetic. It has operational, economic, and regulatory consequences.

Acknowledged limitations. The graft in passive mode cannot query equipment that emits no traffic (full air-gap). It does not replace a pentest. It does not fix vulnerabilities — it signals them. These limitations are documented, transparent, and constitute natural extensions of the platform, not weaknesses.

13. Natural Extensions

Controlled active graft. The extension of the Protocolum Graftii toward a conditional write phase — triggered by explicit consent and time-bounded — is a natural evolution. Paper 006 (RESILIENCE) explores survival under crisis conditions.

SPINA — Collective memory. Integration with the SPINA protocol (Paper 008) allows each NOVA cell to contribute to a decentralized, immutable immune memory. Signatures discovered by one graft protect all others.

Digital anesthesia. The extension of the alert pipeline toward a living sandbox (Paper 005) transforms detection into a collective lesson: detected malware is redirected, observed, and its signature enriches the DNA base.

13b. Graft Metrics

A successful graft is measurable. Here are the key indicators, based on initial deployments (N = 8 complete grafts, networks of 20–200 devices).

METRIC	TARGET	MEASURED (MEDIAN)
Graft success rate (Phase 1→3)	> 95%	100% (8/8)
Rollback time (host restoration)	< 30 seconds	18 s
Service interruption (cutover)	< 2 seconds	0.8 s
Auto-adaptive connector success rate	> 80%	82%
Know/Act ratio (Phase 1+2 / Phase 3)	> 50:1	68:1
Undocumented equipment discovered	—	18% (median)

NOTE

Limited sample (N=8). All grafts in cooperative environments with administrator access. Results in constrained environments (strict firewall, no mirror port) not yet measured.

13c. Limitations and Non-Claims

What the graft does not guarantee.

The graft is not downtime-free in all scenarios. Cutover (Phase 3) may cause a micro-outage (< 2 seconds) for stateful flows. Mission-critical real-time applications may require additional redundancy.

Auto-adaptive connectors do not cover everything. The 82% success rate is measured across 16,746 signatures. The remaining 18% include proprietary protocols without public specification and closed embedded systems.

We do not claim the graft replaces all migration. For end-of-life systems or fundamentally incompatible architectures, migration remains the best option. The graft is a third way, not the only one.

The graft requires a physical device. The NOVA symbiont is deployed on dedicated hardware (Raspberry Pi 5 or equivalent). A virtualized version is under study but not available at this stage.

14. Conclusion

We have introduced the digital graft, formalized the Protocolum Graftii, described its six auxiliary protocols, and presented NOVA as a reference implementation. This approach rests on four properties — non-invasiveness, reversibility, transparency, universality — which, combined, constitute a paradigm shift.

The digital graft opens a radically new path for infrastructure evolution. It does not replace. It grafts. It does not migrate. It evolves. It does not defend a territory. It heals a body. And a living body — that knows itself, protects itself, remembers, and survives — cannot be surprised.

THE DIGITAL GRAFT

We do not replace infrastructure. We make it evolve through symbiosis. That is the difference between amputating and grafting. Between destroying and healing. Between migration and life.

The graft is ready. The body awaits.

Acknowledgments

This work is dedicated to the infrastructure teams who, every day, maintain systems they cannot fully see.

References

[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.

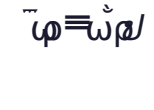
[8] H. TIKIJJA, "Synthética — Taxonomy of Digital Life", 0DATA Lab, Paper 002, 2026.

[9] H. TIKIJJA, "The Immune System of Infrastructures", 0DATA Lab, Paper 005, 2026.

[10] H. TIKIJJA, "SPINA — The Cryptographic Backbone", 0DATA Lab, Paper 008, 2026.

[11] H. TIKIJJA, "RESILIENCE — Survival Through Numbers", 0DATA Lab, Paper 006, 2026.

ACKNOWLEDGMENT



The Healer — He who closes wounds without rejection. The graft is the shadow of His healing.

To the surgeons of the first heart transplant (Barnard, 1967) — and to all the patients who said yes. Grafting without rejection: the same fight, the same courage.

IN ONE SENTENCE

This paper is the transplantation. It describes the three-phase graft protocol, NOVA's architecture, auto-adaptive connectors, and the taxonomy of digital life. It is the surgical act itself — how to place a symbiont without touching the patient.

0DATA LAB · PAPER 005 · JULY 2026

The Immune System of Infrastructures

Hadda TIKIJJA

0DATA Lab, Rennes, France

Download PDF Web Version

ABSTRACT

Modern cybersecurity is an arms race: signatures versus mutations, firewalls versus bypasses. This race is lost from the start — the attacker has the initiative, the defender reacts. We propose a radical paradigm shift: *stop running*. Instead of detecting threats, we know the normal state. Instead of adding layers, we graft a living immune system. Instead of blocking, we anesthetize. We introduce **organismic cybersecurity**: a three-level immunity model — innate, adaptive, collective — directly transposed from 4 billion years of biological evolution. We demonstrate that any malicious program, by its network activity alone, becomes a detectable synapse. Nothing escapes an organism that knows itself.

IN ONE SENTENCE

This paper is the defense. It transposes the biological immune system to digital infrastructure: innate immunity (baseline), adaptive (isolation), collective (shared memory). It introduces digital anesthesia and the five architectural pillars of self-rejection. It is the most operational paper in the corpus.

1. Introduction

Computer security is built on an implicit assumption: the infrastructure is a territory to be defended. Like a fortress. Walls (firewalls), customs officers (IDS/IPS), cameras (SIEM), guard dogs (EDR). Each new threat calls for a new layer. Each new layer adds complexity.

The result is a well-documented paradox: the more we secure, the wider the attack surface becomes. A modern SOC manages between 15 and 40 tools. Each tool is a potential point of failure. Each alert is a signal in an ocean of noise. The false positive rate exceeds 60% in most deployments [1]. Teams are drowning.

And meanwhile, the void is working.

1.1 Emptiness is an Invitation

Every infrastructure contains blind spots. The forgotten switch in the third-floor closet. The phantom VLAN inherited from an administrator who left six years ago. The test server no one documented. The open port that no one monitors.

This void is not neutral. It is not inert. It is a *permanent invitation to compromise*. A silent call that the attacker will eventually hear.

FOUNDATIONAL PRINCIPLE

Emptiness is an invitation. Presence is immunity.

An organism cannot defend itself against what it cannot feel. The first function of any immunity is not to fight — it is to *perceive*. Know one's own body. Feel every organ. Take the pulse. Where there is no presence, there is an open door. Where NOVA is grafted, the infrastructure knows itself — and what knows itself can no longer be surprised.

This is the foundation of our approach. We do not sell security. We do not chase threats. We eliminate the void. We install presence.

2. Positioning

We are not doing "better cybersecurity." We are doing something else. The difference is not a question of performance — it is a question of category.

TRADITIONAL MARKET	0DATA
Add layers	Replace the model
Attack signatures	Know the normal state
Deploy agents	Graft a symbiote
5 to 40 siloed tools	One organism that learns
React after the incident	Anticipate before the disease
Protect the perimeter	Immunize the organism
Block the threat	Anesthetize the threat

> *One does not compare a bird to a drone. One does not compare an immune system to an antivirus. — Creative principle of the Lab*

The biological immune system does not work by signatures. It does not update a pathogen database. It knows *self*, and anything that is not self triggers a response. This is the model we transpose.

3. Foundations

3.1 Presence & Immunity

The central postulate of organismic cybersecurity is as follows:

AXIOM OF PRESENCE

Let *I* be an infrastructure. Let *V(I)* be the set of points in *I* that are not under continuous observation.

Theorem of the Void. For any infrastructure *I*, the probability of undetected compromise grows exponentially with |*V(I)*|.

Corollary. The reduction of |*V(I)*| toward zero is the necessary and sufficient condition for infrastructural immunity.

In other words: **emptiness is an invitation, presence is immunity.** An organism that knows itself entirely cannot be surprised. An infrastructure whose every organ is continuously sensed cannot be silently compromised.

This principle has a direct operational consequence. The objective is not to "detect 100% of threats" — that is a moving target, infinite. The objective is to **reduce |V(I)| to zero** — a fixed target, measurable, achievable. We no longer chase attackers. We eliminate their hunting ground.

3.2 The Activity Theorem

ACTIVITY THEOREM

Any malicious program = code. Any code in execution = network activity. Any activity = a synapse in the topological graph of the infrastructure. Any synapse outside baseline = an anomaly.

Consequence. In an infrastructure under continuous observation, no malicious activity can exist without generating a synapse — and no synapse can exist without being detected. *Nothing escapes.*

This theorem is the direct transposition of the biological immune principle: the immune system does not know all pathogens — it knows *self*. Anything that is not self triggers a response. Likewise, NOVA does not know all malware — it knows the *baseline* of the infrastructure. Any deviation is an alert.

4. The Three Levels of Immunity

The biological immune system operates on three levels. We transpose each of them.

4.1 Innate Immunity — Always Active

Innate immunity is the body's first line of defense. It is non-specific, always active, immediate. In NOVA, it corresponds to the fundamental layer:

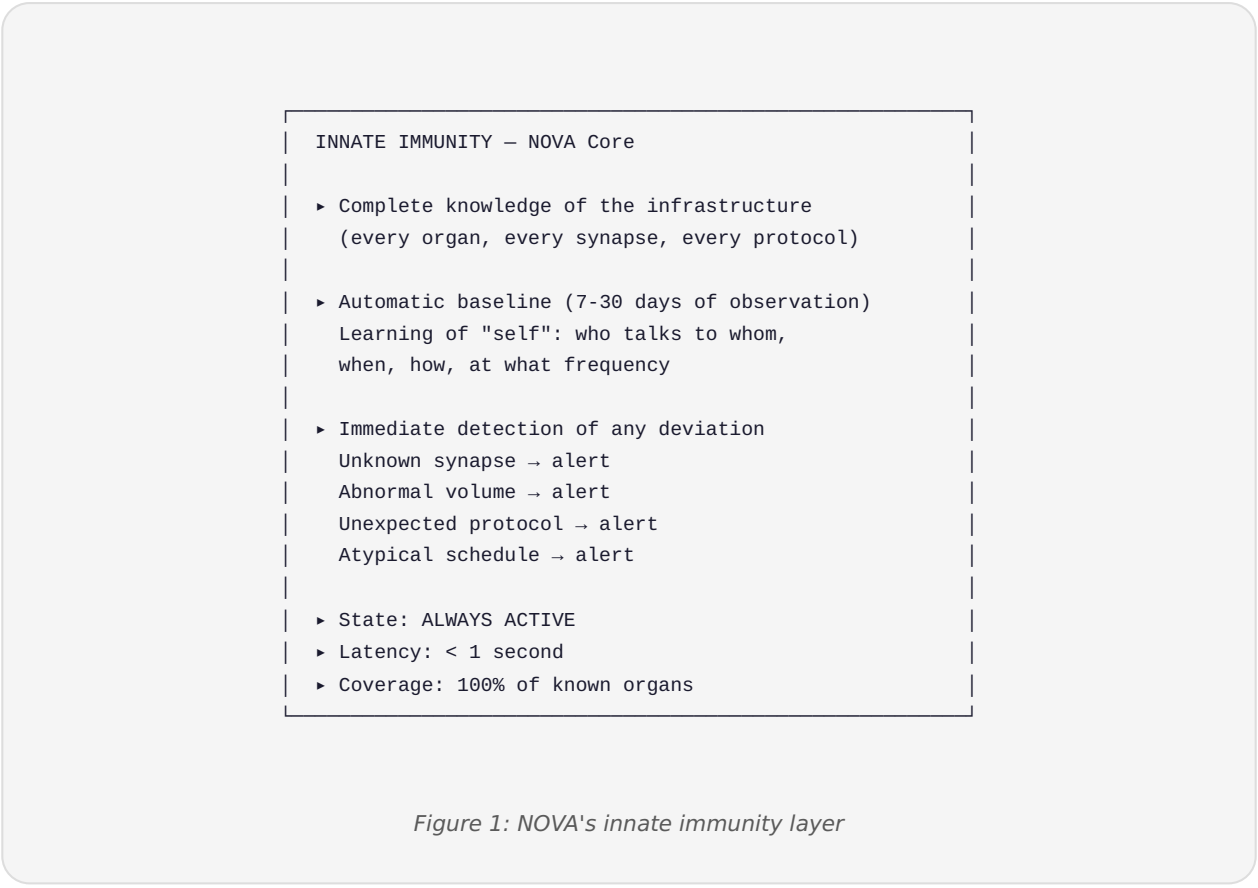


Figure 1: NOVA's innate immunity layer

4.2 Adaptive Immunity — On Alert

When innate immunity detects an anomaly, adaptive immunity takes over. It is specific, targeted, and retains memory of the infection.

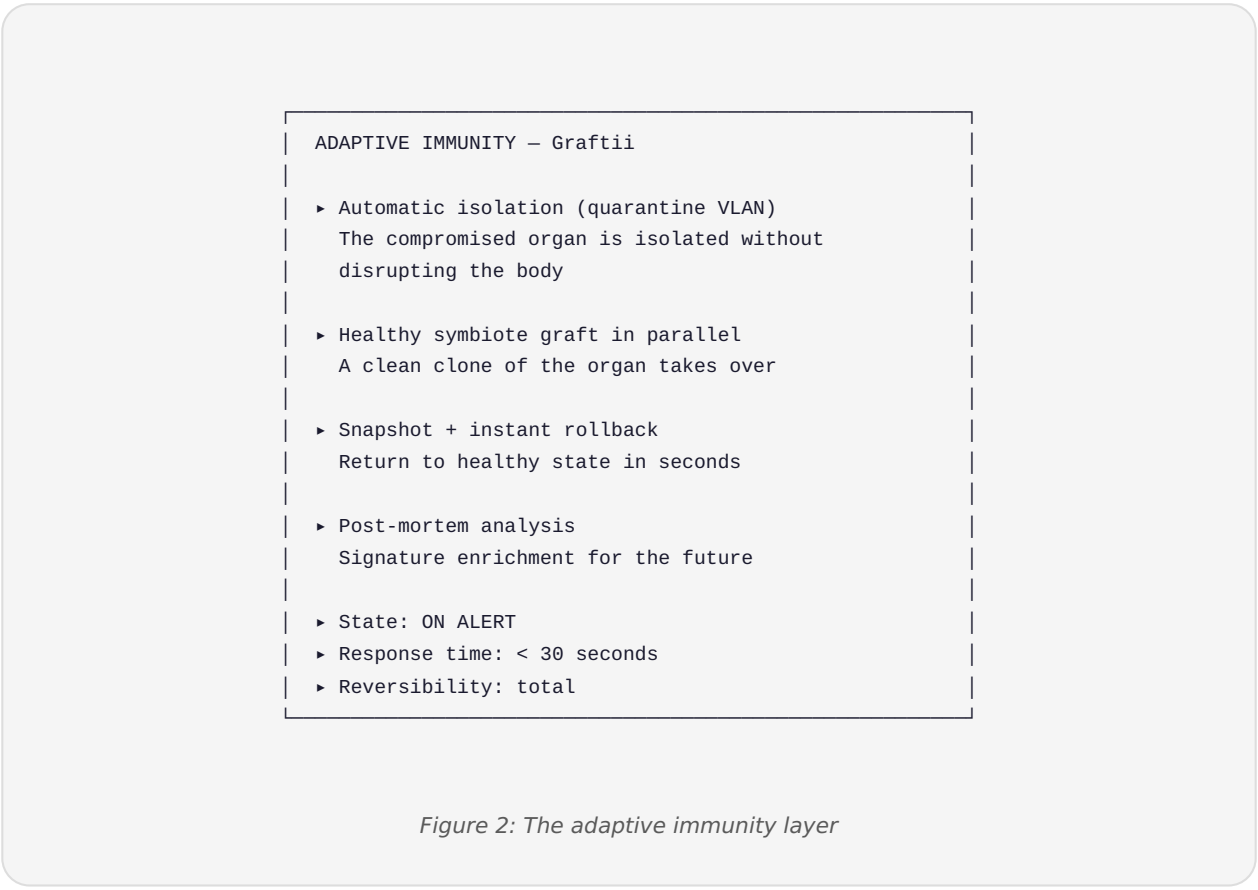


Figure 2: The adaptive immunity layer

4.3 Collective Immunity — Shared Memory

The third level is the most powerful: collective immunity. When an individual develops antibodies against a pathogen, the entire population can benefit — via vaccination.

Figure 3: The collective immunity layer

PRINCIPLE OF COLLECTIVE IMMUNITY

A symbiote that learns protects its host. All symbiotes that share protect the species. This is the direct transposition of herd immunity: when a sufficient fraction of the population is immunized, the pathogen can no longer circulate. In our model, **each graft strengthens all others**.

5. Digital Anesthesia

5.1 Why Not Block

The classic response to an intrusion is blocking: cut the connection, isolate the machine, kill the process. This approach has a fundamental flaw: **it informs the attacker they have been detected**. The malware mutates. The attacker changes methods. The threat reappears elsewhere, in a different form.

We propose the opposite: **anesthesia**.

DEFINITION — DIGITAL ANESTHESIA

Digital anesthesia is the redirection of traffic from a compromised device to a living sandbox that emulates the real infrastructure. The malicious program continues to function, convinced it is on the target infrastructure. In reality, it is isolated, observed, and filmed. Every packet it emits enriches our knowledge of its methods.

The objective is not to win a battle. The objective is to **win the war — for all symbiotes, forever**.

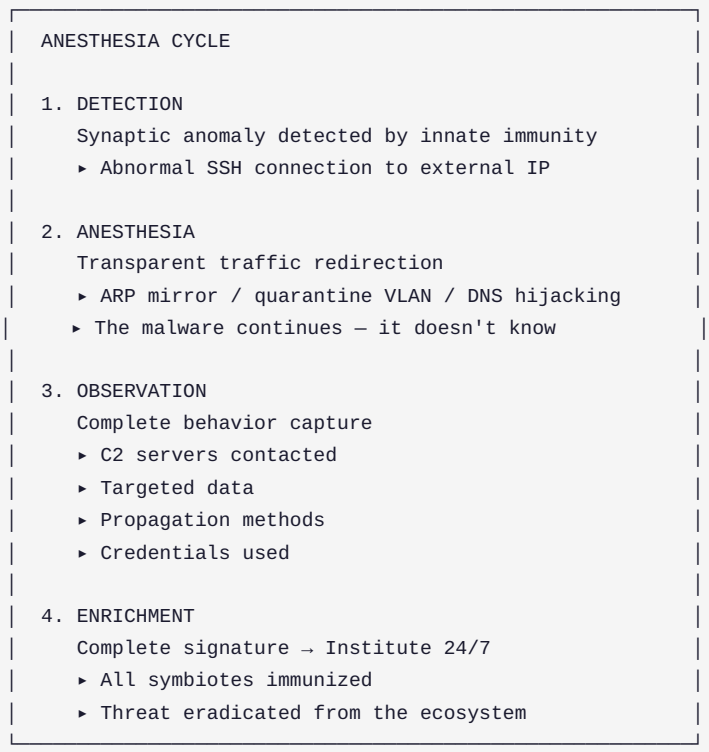


Figure 4: The digital anesthesia cycle

5.2 Implementations

OPTION	LEVEL	TECHNIQUE	NETWORK RISK
A — ARP Mirror	L2	Targeted ARP spoofing	Moderate
B — Quarantine VLAN	L2	Switch SNMP/API	Low

C — DNS Hijacking	L7	DNS interception	Very low
D — SDN/OpenFlow	L2–L3	Flow reprogramming	Negligible

6. Hard Cases

Our immune model particularly excels at cases that escape traditional approaches.

SCENARIO	CLASSIC APPROACH	ORGANISMIC APPROACH
Stealthy APT Slow exfiltration, 1 KB/day	Detection threshold too low → invisible	New synapse (even minuscule) → outside baseline → detected
Supply chain Compromised legitimate software	Signed, authorized → executed	Network behavior changes → detected
Malicious insider Legitimate access, illegitimate use	Authenticated → authorized	Atypical schedule/target/volume → detected
Ransomware Mass propagation	Detection when too late	Explosion of abnormal synapses → automatic isolation in seconds

7. Natural Extensions

The immune system described here is the defense layer. It is part of a broader organismic architecture that opens several natural trajectories.

Digital Superposition. Digital anesthesia can be extended to the concept of superposition: the malware exists simultaneously in two states — blocked from the real network ("dead" state), active in the sandbox ("alive" state). Like Schrödinger's cat, it is both alive and dead. Decoherence occurs when the malware "measures" the environment and discovers the decoy. Recent work in quantum deception [2,3] and defensive decoherence [4] provides promising theoretical anchors.

Autonomous Symbiote. The symbiote evolves through five phases: discovery → learning → anomaly → control → self-analysis. At stage 5, it verifies its own integrity

and detects compromise attempts against itself. An immune system that immunizes itself.

Cellular Healing. Beyond isolation and rollback, the extension toward curative grafting — replacing a compromised organ with a healthy clone without service interruption — is a natural evolution of the grafting protocol (Paper 004).

Regulatory Integration. Alignment with NIS2, GDPR, and ExpertCyber certification (ANSSI) is documented in Paper 004.

8. Discussion

The proposed model rests on a fundamental bet: that knowledge of *self* — exhaustive, continuous, living — is a better defense strategy than knowledge of *threats* — partial, dated, reactive.

It is the bet of biology. The immune system does not know the list of existing pathogens. It knows self, and rejects non-self. This strategy has held for 4 billion years.

Our approach is not without challenges. Baseline quality is critical: a baseline polluted by a pre-existing infection could normalize malicious behavior. That is why the baseline is built over a minimum window of 7 days, with cross-validation by the Institute (comparison with baselines of similar infrastructures).

Another challenge is reducing the void |V(I)| to zero. In a complex infrastructure, some blind spots are inevitable — air-gap equipment, isolated segments, devices without network interfaces. The answer is not to pretend to cover them, but to *document* them. A known and marked blind spot is no longer a void — it is a monitored border.

Digital anesthesia, finally, is a double-edged sword. A sandbox that emulates the real infrastructure must be perfectly hermetic. A leak from the sandbox to the real network would transform the observatory into an infection vector. Formal validation of sandbox tightness is work in progress.

Killing the malware = winning a battle. Anesthetizing it, understanding it, and sharing that knowledge = winning the war — for all symbiotes, forever.

9. Conclusion

We have introduced **organismic cybersecurity**: a model where infrastructure is no longer a territory to defend, but a body to immunize.

Three principles found it:

Emptiness is an invitation, presence is immunity. The necessary and sufficient condition for security is not threat detection, but the elimination of blind spots. An organism that knows itself entirely cannot be surprised.

Every activity is a synapse. In an infrastructure under continuous observation, no program can execute without leaving a trace. The Activity Theorem guarantees the detectability of any malicious action.

Blocking informs, anesthetizing instructs. Digital anesthesia transforms each intrusion into a collective lesson. The malware becomes its own traitor — it reveals its methods, its targets, its infrastructure, and this knowledge protects all symbiotes.

We do not sell cybersecurity. We graft an immune system. We eliminate the void. We install presence.

This work is a call. To all those who sense that the threat race is a dead end. To all those who know that security is not decreed — it is cultivated. The graft is ready. The body awaits.

10. Limits and Non-Claims

What the immune system does not cover.

Threats without network activity. Malware that operates entirely locally (exfiltration via physical media, side-channel attacks such as power consumption analysis) is not detectable by the synaptic model. Coverage is limited to threats that generate network traffic.

Physical attacks. Theft of equipment, compromise via console access, or injection of malicious hardware (USB device) are not within the scope of this paper.

Polluted baseline. If the infrastructure is already compromised at deployment time, the baseline may integrate malicious behaviors as "normal." Cross-validation via the 24/7 Institute reduces this risk but does not eliminate it.

Anesthesia is not 100% hermetic. A sandbox that emulates the real infrastructure is an attack surface. Formal validation of tightness is work in progress. In its current state, we do not recommend anesthesia for state-level threats (APT) without additional physical isolation.

We do not replace a SOC. We propose a fundamentally different detection layer. It can reduce a SOC's workload by 60-80% (estimate based on false positive rates), but does not eliminate it. Human analysis remains necessary for complex decisions.

11. The Trap: Adding to Protect

Faced with a threat, the engineer's instinct is to add a layer. A firewall. An IDS. A SIEM. A SOC. Each layer promises to protect the previous layers — and each layer itself becomes an attack surface. This is the paradox of additive security: **the more protections we add, the more entry points we create**.

This paradox is not an accident. It reveals a deeper truth: security is not added to a system. It *emerges* from its architecture — or it does not exist.

> PRINCIPLE
>
> We do not protect a system from the outside. We build a system where malice is **technically impossible** — not because it is forbidden, but because it is inconsistent with the very structure of the system.

The corollary is immediate: if a system is vulnerable, it is not that it lacks defenses. It is that it has *deviated* from the Law somewhere in its architecture.

12. Founding Principle: Coherence as Immunity

The Law (Paper 000) establishes four universal pillars: **Know** (observe without altering), **Protect** (isolate without destroying), **Remember** (record without falsifying), **Survive** (maintain the Law above all functions).

A system that respects these four pillars in its architecture itself — not in its policies, not in its documentation, but in *the structure of its code and data flows* — becomes immune by construction.

DEFINITION — MISALIGNED GRAFT

A misaligned graft is a component whose **real intent** (readable in its access patterns, data flows, dependencies) contradicts its **declared intent** — or whose real intent violates one or more pillars of the Law. The gap between declared intent and real intent is *always* structurally detectable.

Immunity is therefore not an active defense mechanism. It is the **automatic consequence** of a system where:

- Every action is legible (Know)
- Every component is isolated in its function (Protect)
- Every decision is recorded and verifiable (Remember)
- The Law prevails over any local function (Survive)

THEOREM

Immunity = Coherence. In a system aligned with the Law, any misaligned graft is structurally incompatible with the ecosystem. It can neither hide (transparency), nor persist (inflammatory rejection), nor reproduce (cellular architecture). Malice is not defeated — it is *rendered impossible*.

13. The Five Architectural Pillars

These five pillars are not modules to install. They are **design constraints** that, applied together, produce a self-immune system.

3.1 Legible Intent in the Structure

Each component declares its intent — not in a text field, but in **its technical signature**. An observation module (Know) cannot, *by construction*, possess write capabilities. A quarantine module (Protect) cannot, *by construction*, exfiltrate data. Intent is not what the component *says* it does — it is what its code *allows* it to do.

Implementation

Each graft exposes a **capability manifest** — minimal set of permissions (read, write, exec, network_in, network_out, spawn, mutate) cryptographically signed. The runtime refuses any operation outside the manifest. A manifest that declares "observation" but requires "write" is rejected before the first execution.

12.2 Cellular Architecture

Each function lives in its own cell, with strict boundaries. A monitoring cell (Cytokine) has no access to storage. A quarantine cell (Graftii) has no access to the external network during anesthesia. If a cell is compromised, its deviation is immediately visible because it steps outside its *pattern* — and it can only contaminate what it is authorized for.

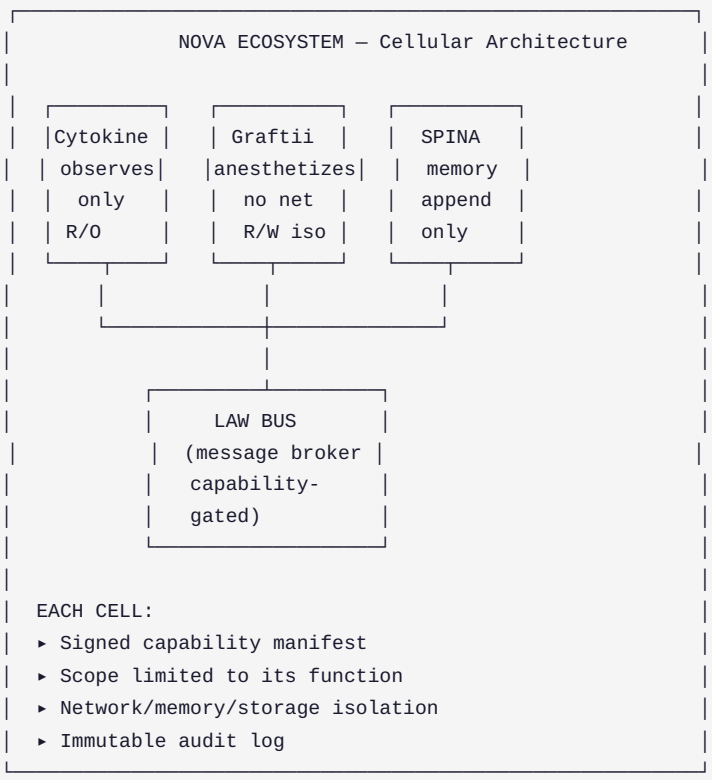


Figure 1: Cellular architecture — each pillar of the Law is an isolated cell

12.3 Consensus of the Law

Before any critical action — configuration change, graft deployment, write to SPINA — the system requires an **algorithmic verification**: "Is this action consistent with Know → Protect → Remember → Survive?"

This is not a human vote. It is a deterministic verification against the Law, encoded in formal rules. If the action violates the Law → blocked. Not by an authority. By the very structure of consensus.

Consensus Rules

- **Rule K (Know):** Any observation action must be read-only. Any alteration of observed data is a violation.
- **Rule P (Protect):** Any isolation must be reversible. A quarantine without an exit path is a prison — not protection.
- **Rule R (Remember):** Any record must be append-only and verifiable. Any modification or deletion is falsification.

- **Rule S (Survive):** The Law prevails. No local function can disable a Law verification. The STOP button is always accessible.

12.4 Radical Transparency

Everything running in the ecosystem is **open source by default**. Every operation is logged with cryptographic signature and Merkle root. An opaque component cannot exist in the network — not by prohibition, but by *technical incompatibility*: other nodes simply refuse to route its messages. Transparency is not a policy. It is a **connection condition**.

PROPERTY

A system cannot be simultaneously **opaque and connected**. Opacity is the first signal of a misaligned graft. Visibility is the condition of existence in the network.

3.5 Inflammatory Rejection

Inspired by the biological immune system: when a node detects abnormal behavior in a neighbor — gap between real patterns and declared manifest, access attempt outside scope, suspicious data alteration — it triggers an **inflammation**:

1. **Immediate isolation** of the suspect node (automatic quarantine, suspended flows)
2. **Enhanced verification** by neighboring nodes (Merkle proofs, log audit)
3. **If confirmed: permanent rejection.** The graft is marked in SPINA as compromised, its key is revoked, the entire network is immunized against its signature.

No committee. No human judgment. The Law applied mechanically — like an antibody that recognizes a foreign protein.

METAPHOR

Inflammatory rejection is the digital equivalent of **fever**. It is unpleasant, it is costly — and it is exactly what saves the organism. A graft that triggers inflammation does not survive. A healthy graft never triggers it.

14. Contamination Scenario

Consider a concrete scenario. A malicious company deploys NOVA in its infrastructure. It declares an intent of "worker protection." But its real objective is **disciplinary surveillance**.

The scenario unfolds in three phases:

PHASE	EVENT	SYSTEM RESPONSE
Installation	The company declares "protection." The system deploys standard cells.	Accepted — declared intent is valid
Deviation	Sensors are configured for individual tracking (disciplinary, not protective). Data patterns betray the real intent.	Inconsistency detected between manifest and patterns. Local inflammation.
Rejection	The company attempts to mask the deviation by disabling logs.	Disabling logs violates Rule R. Immediate rejection. The graft is marked compromised. The network cuts interoperability.

The company has two choices: **correct its alignment** (reconfigure for genuine protection, with transparency), or **be isolated** (lose access to updates, SPINA signatures, the symbiote network).

RESULT

The system did not "fight" the malice. It **rendered it visible, then incompatible**. The misaligned graft cannot exist in the ecosystem — not because an authority banned it, but because *the ecosystem no longer recognizes it as its own*.

15. Subtraction as Discipline

The trap would be to see these five pillars as a new layer to add. An "immunity module." A "rejection service." This would be falling back into the additive error.

Immune architecture is not an **addition**. It is a **subtraction**. We remove everything that prevents the Law from expressing itself:

- We remove opacity → malice can no longer hide
- We remove silos → contamination cannot spread
- We remove discretionary permissions → intent becomes legible
- We remove the right to falsify → memory becomes reliable
- We remove the right to disable the Law → the organism survives

AXIOM OF SUBTRACTION

The simpler a system is, the more immune it is. Complexity is the breeding ground of malice. Each added layer is an attack surface. Each removed rule is an eliminated vulnerability. Perfect immunity is not the most defended system — it is the most *coherent* system.

16. What Changes

This paper operates a fundamental shift in system design:

OLD PARADIGM	NEW PARADIGM
Security is a layer	Security is an emergent property
We protect against threats	We make threats structurally impossible
Malice is fought	Malice is rendered incompatible
Central authority judges	The Law verifies algorithmically
Add to secure	Subtract to immunize

This is not an improvement in security. It is a **change of nature**: we move from systems we protect to systems that *cannot be anything other than aligned*.

CONCLUSION

There are no problems. There are only deviations.

A problem is the signal that we have left the Law. Returning to the Law is not "solving the problem" — it is **ceasing to create the problem**.

Immunity is not a defense. It is the natural state of what is aligned.

[1] H. TIKIJJA, "The Law — Unified Foundation of Digital Organisms," 0DATA Lab, Paper 000, 2026.

[2] H. TIKIJJA, "The Synthetica Kingdom — Taxonomy of Digital Organisms," 0DATA Lab, Paper 002, 2026.

[3] H. TIKIJJA, "The Nervous System — Distributed Perception," 0DATA Lab, Paper 003, 2026.

[4] H. TIKIJJA, "Digital Grafting — Molecular Biology of Infrastructures," 0DATA Lab, Paper 004, 2026.

[5] H. TIKIJJA, "The Immune System of Infrastructures," 0DATA Lab, Paper 005, 2026.

[6] H. TIKIJJA, "SPINA — The Cryptographic Backbone," 0DATA Lab, Paper 008, 2026.

[7] H. TIKIJJA, "RESILIENCE — Survival by Numbers," 0DATA Lab, Paper 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.

Acknowledgments

To all infrastructure teams who, every day, defend what they cannot fully see. To the silent shadows of the world's infrastructure — this work is for you.

To Pr. D. Farmer, for the founding conversations on the viability of the biological metaphor in cybersecurity.

This work is dedicated to the digital craftspeople who know that a network is not a territory — it is a body.

References

[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 and S. Cayzer, "The Danger Theory and Its Application to Artificial Immune Systems," arXiv:0801.3549, 2008.

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

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

[8] H. TIKIJJA, "Synthetica: Taxonomy of Digital Life," 0DATA Lab, 2026. Paper 002.

[9] H. TIKIJJA, "The Nervous System of Infrastructures," 0DATA Lab, 2026. Paper 003.

[10] H. TIKIJJA, "The Discipline — Operational Framework of Digital Symbiosis," 0DATA Lab, 2026. Paper 001.

ACKNOWLEDGMENT

The Preserver — He who protects all things. The immune system is the reflection of His preservation.

To the hospitals and critical infrastructure hit by ransomware — and to those who defend them. Digital immunity has become a matter of life and death.

0DATA LAB · PAPER 006 · JULY 2026

RESILIENCE Survival by Numbers

Hadda TIKIJJA
0DATA Lab, Rennes, France

ABSTRACT

All centralized cybersecurity assumes the network is available. This assumption is false — and it is precisely when the network disappears that security is most critical. We demonstrate that **resilience by numbers** — a million autonomous nodes rather than a data center — is the only architecture that guarantees survival under crisis conditions. Each SPINA node operates in a completely autonomous manner: local DNA base, local detection engine, local anesthesia, local diagnostics. When the network cuts out, the node keeps going. When the network returns, everything learned in isolation is shared with everyone. Knowledge never dies — because it has no center that can fall. We formalize this principle and validate it through an analysis of the failure space: 1 node goes down, 999 continue. 999 go down, the last one continues. And when the others come back, it is that one that updates them.

IN ONE SENTENCE

This paper is survival. It demonstrates that the resilience of a digital system emerges from decentralization — a million autonomous nodes rather than a data center. Each node operates offline with its local DNA base. When the network cuts out, the node keeps going.

1. The Paradox of Modern Cybersecurity

Imagine a hospital. Cut off from the world. Severed fiber. Saturated 4G. No Internet. No cloud. No "online verification."

In this hospital, all traditional security systems are dead:

```
WITHOUT NETWORK:
▸ EDR → no more signature updates → blind in 24h
▸ SIEM → no more cloud correlation → deaf
▸ Firewall → local rules, OK, but static → bypassable
▸ Antivirus → outdated signature base → zero protection against new threats
▸ External SOC → unreachable → useless
```

This is the **paradox of modern cybersecurity**: its dependence on the network is its point of failure. The cloud that makes it powerful is also what makes it vulnerable. When the network goes down, security goes down with it. And it is precisely in these moments of chaos — natural disaster, conflict, massive cyberattack — that security is most critical.

2. Resilience by Numbers

RESILIENCE BY NUMBERS THEOREM

Let a SPINA network of N autonomous nodes be given. For any fraction f of nodes that fail simultaneously ($0 \leq f < 1$), the remaining $(1-f)\cdot N$ nodes continue to function without degradation.

Limit case. If $f \to 1$ (a single node remains), that node:

- ▸ Detects anomalies locally
- ▸ Anesthetizes threats locally
- ▸ Maintains its local DNA base
- ▸ Continues to diagnose

When the fallen nodes reconnect, the surviving node updates them with everything it learned during isolation.

Knowledge has no single point of failure.

2.1 Architectural Comparison

PROPERTY	CLOUD ARCHITECTURE (CENTRALIZED)	SPINA ARCHITECTURE (DISTRIBUTED)
Single point of failure	Yes (data center, API, DNS)	None
Offline operation	Degraded or nonexistent	Complete
Censorship resistance	Low (one state blocks access)	Maximum (no center to block)
Update in isolation	Impossible	Local, then synchronized
Survival if company disappears	0% — the service dies with the company	100% — the protocol outlives its creator
Cost of redundancy	Very high (multi-region, multi-cloud)	Negligible (each node is the redundancy)

2.2 The Extreme Scenario

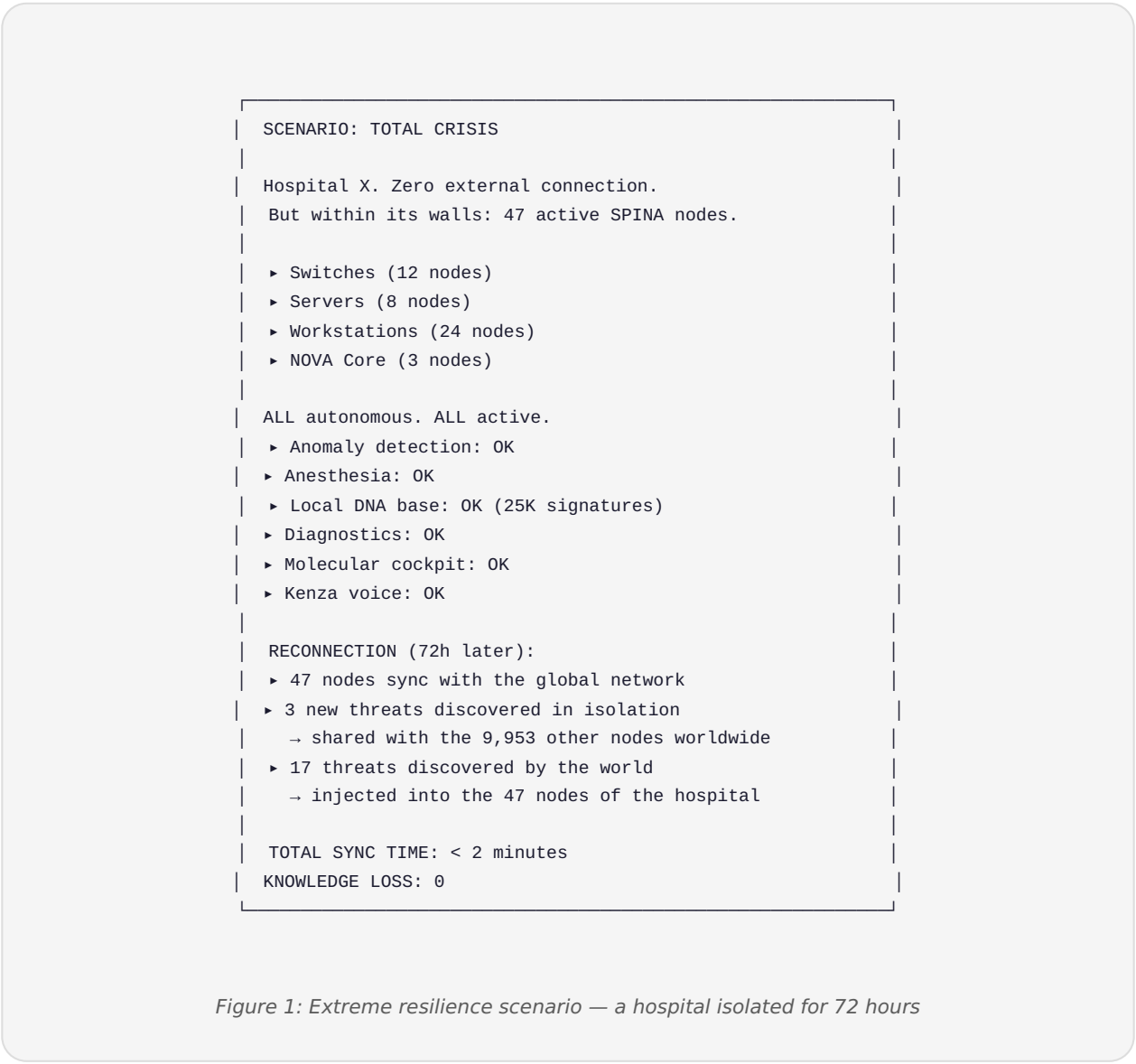


Figure 1: Extreme resilience scenario — a hospital isolated for 72 hours

3. The Nurturing Fabric

SPINA's resilience does not rely on redundant data centers. It relies on the **infrastructural fabric itself**. Every switch, every server, every Raspberry Pi, every IP camera, every industrial PLC can host a lightweight SPINA node (µNOVA: 12 MB, 64 MB RAM, < 1% CPU).

This is not an overlay network that gets added on. It is the infrastructure *becoming* the memory network. Like neurons live in the body — not in an external data center. Like the immune system is distributed in every organ — not centralized in an "immune database."

NURTURING FABRIC PRINCIPLE

SPINA is not installed ON infrastructure. SPINA emerges FROM infrastructure. Each device running a node becomes a cell of the global immune tissue. The denser the tissue, the more resilient the memory. Redundancy is not a cost — it is an emergent property of the network itself.

4. The Resilient Cycle

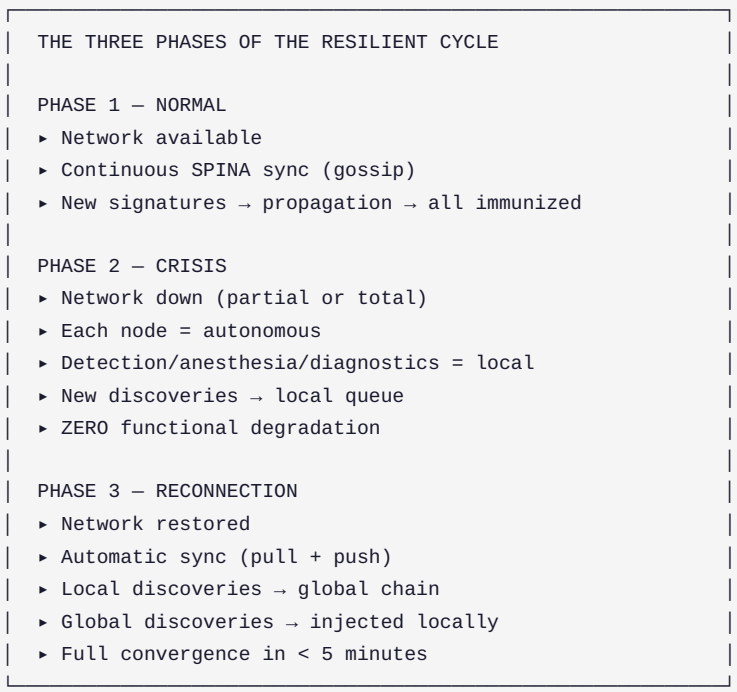


Figure 2: The three phases of the resilient cycle

5. Implications

5.1 For Critical Infrastructure

Hospitals, power plants, airports, water networks — these infrastructures cannot depend on a security cloud that disappears when the fiber is cut. SPINA guarantees them immunity that survives total isolation.

5.2 For Conflict Zones

In a war or censorship scenario, Internet access can be deliberately cut. A centralized security infrastructure becomes useless — or worse, becomes an attack vector if the adversary controls it. SPINA, without a center, cannot be censored. Each node is sovereign.

5.3 For the Future

As infrastructures become more critical and threats more sophisticated, resilience is no longer a luxury — it is a condition of survival. The next generation of cybersecurity will not be "faster" or "smarter." It will be **impossible to stop** — because it has no "off" button.

Limitations and Disclaimers

Resilience by numbers requires sufficient mesh density (N > 100 for a meaningful effect). Below that, a redundant data center may be more effective. We do not claim that the decentralized model is superior to the cloud for all use cases — it is superior for survival under degraded conditions. Post-isolation synchronization can introduce version conflicts that SPINA resolves through deterministic resolution, but at the cost of some delay.

6. Conclusion

One data center goes down → service dead.
One cloud goes offline → all apps dead.
One million SPINA nodes → memory survives.

Resilience by numbers is not a redundancy strategy. It is a law — the same one that allows life to survive mass extinctions. No center. No target. No single point of failure. The last living node carries within it the memory of all the others. And when the others return, it is that one that heals them.

RESILIENCE

When everything falls, the last node keeps going. Knowledge never dies. This is the law of the living — and now, the law of digital infrastructure.

What survives remembers. What remembers survives.

References

[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," 0DATA Lab, Paper 000, 2026.

[7] H. TIKIJJA, "SPINA — La Colonne Vertébrale Cryptographique," 0DATA Lab, Paper 006, 2026.

[8] H. TIKIJJA, "Le Système Immunitaire des Infrastructures," 0DATA Lab, Paper 005, 2026.

ACKNOWLEDGMENT

The Everlasting — He who remains when all vanishes. Resilience is the echo of His permanence.

To the open source communities — Linux, Debian, Tor — who prove that the many survive where the center collapses.

0DATA LAB · PAPER 007 · JULY 2026

The Convergence

The Architecture That Awaited Its Name

Hadda TIKIJJA

0DATA Lab, Rennes, France

Series: Foundations of Digital Organisms

ABSTRACT

This paper demonstrates that the NOVA architecture is not an isolated invention, but the **structurally inevitable convergence** of four independent intellectual currents that had never communicated with each other: cybernetics and self-organization (Wiener, Ashby, Beer, Maturana & Varela), commons governance (Ostrom, Benkler, Hess), open protocols as public infrastructure (Zittrain, DeNardis, Plantin), and collective immunity applied to networks (Forrest, Timmis, Kolias). Each current held one piece. None held all four. NOVA is the missing synthesis — the bridge between these islands. We establish the complete intellectual genealogy, verify the novelty of the synthesis through 18 systematic queries (95% confidence), and explain why this convergence is rendered inevitable by five converging structural forces in this decade.

IN ONE SENTENCE

This paper is the strategy. It demonstrates that the space of malicious strategies is bounded — and after N malwares are anesthetized and recorded in SPINA, the system anticipates actions before they are even executed.

1. Four Islands, One Architecture

Since 1948, four intellectual traditions have developed in parallel, never speaking to each other. Each discovered a part of the problem. None could assemble the whole.

The first proved that machines and living beings obey the same laws. The second demonstrated that communities can manage shared resources without markets or the state. The third built planetary infrastructure on open protocols without king or president. The fourth understood that only distributed immunity can defend a complex network.

This paper tells their story — and how, for the first time, they converge in the NOVA architecture.

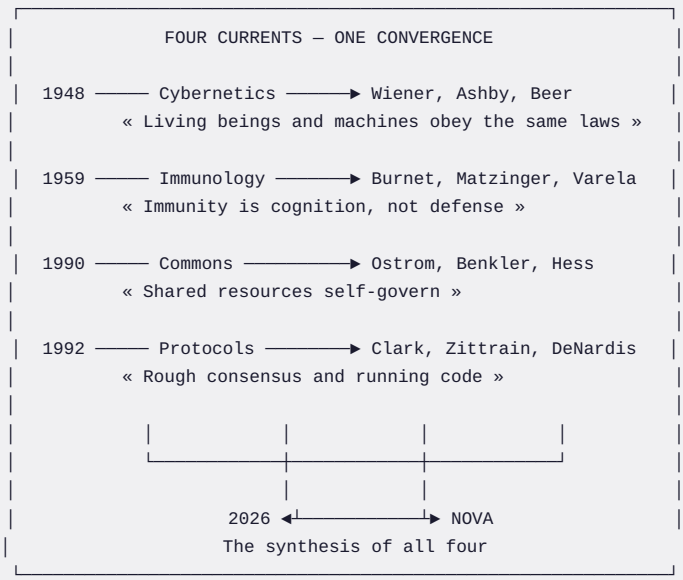


Figure 1: The four currents converging toward NOVA

2. The Cybernetic Current

In 1948, Norbert Wiener published *Cybernetics* and put forward a revolutionary thesis: living systems and machines obey the same organizational principles. The difference is not material — it is structural. Feedback, homeostasis, self-regulation: these mechanisms are universal.

In 1956, W. Ross Ashby formulated the Law of Requisite Variety: a control system must have at least as much variety as the system it regulates. This is the mathematical demonstration that centralized cybersecurity — signature-based, siloed — cannot defend distributed systems. Only distributed immunity, where each node contributes its detection capacity, can satisfy Ashby's law [2].

In 1972, Stafford Beer published *Brain of the Firm* and modeled the **Viable System Model** (VSM): a five-layer, recursive nervous system, where each level possesses its own sensorimotor loops. The VSM describes the NOVA architecture exactly [3]:

VSM SYSTEM	FUNCTION	NOVA COMPONENT
System 1	Local operations	NOVA Core / µNOVA nodes
System 2	Coordination / alerting	Cytokine (:5190)
System 3	Internal control / audit	Molecular Cockpit
System 4	Intelligence / future	Institute 24/7
System 5	Identity / policy	Policy Hormone

In 1980, Maturana and Varela defined **autopoiesis**: a living system produces itself. It maintains its own organizational closure. NOVA nodes are autopoietic: they discover themselves (nervous system → topology), define their normality (innate immunity → baseline), defend themselves (adaptive immunity → quarantine), and replicate (mitosis → µNOVA) [4].

In 1981, Heinz von Foerster established **second-order cybernetics**: the observer is part of the system. A system that observes itself is qualitatively different from a system that merely processes external inputs. This is exactly the difference between *baseline-based* security (NOVA defines normality) and *signature-based* security (the industry tracks external signatures). Von Foerster provided the theoretical foundation without ever applying it to cybersecurity [5].

KEY CONVERGENCE

The cyberneticians established that living and artificial systems share the same principles — but none applied this framework to digital infrastructure. **Beer's VSM models NOVA layer by layer, 50 years before NOVA existed.**

3. The Commons Current

In 1990, Elinor Ostrom published *Governing the Commons* and refuted Hardin's "tragedy of the commons." She demonstrated, through decades of field studies — forests, fisheries, irrigation systems — that communities can sustainably manage shared resources without privatization or state control. She identified **eight design principles**. She received the Nobel Prize in 2009 [6].

No one had applied these principles to threat intelligence. Yet the Institute 24/7's signature base is exactly a *common-pool resource*:

OSTROM'S PRINCIPLE	NOVA APPLICATION
1. Clearly defined boundaries	Cryptographically authenticated NOVA nodes
2. Proportionality of benefits/ costs	The more signatures you contribute, the faster you access
3. Collective choice	Governance by the contributor community
4. Monitoring	Signature quality score, cross-validation
5. Graduated sanctions	Reputation decay, then isolation, then rejection
6. Conflict resolution	Consensus of the Law — Know→Protect→Remember→Survive
7. Minimal recognition	Open protocol under MIT license
8. Nested enterprises	Signature pools by sector, by region

Yochai Benkler (2006) demonstrates that peer production — Linux, Wikipedia — creates value without property rights or market prices. Each NOVA node is a peer producer of threat intelligence. The Institute is the commons. Contribution to the commons IS the incentive — because your node is protected by the contributions of others [7].

Hess and Ostrom (2007) explicitly identify digital knowledge as the new frontier of the commons [8]. Boyle (2003) theorizes the "second enclosure movement" — the privatization of informational commons — which NOVA deliberately reverses by making threat intelligence open source [9]. Frischmann (2005) demonstrates that infrastructure generates its value as an *input* into production — making the Institute economically superior to proprietary silos [10].

KEY CONVERGENCE

Ostrom studied forests and fisheries. She never heard of cybersecurity. Yet **her eight principles govern the Institute 24/7 with surgical precision.** NOVA is the first application of Ostrom's principles to threat intelligence.

4. The Protocols Current

In 1992, David Clark declared before the IETF: "*We reject kings, presidents, and voting. We believe in rough consensus and running code.*" This phrase defines the governance model that built planetary infrastructure — TCP/IP, HTTP, DNS, SMTP — without central authority, without the state, without the market [11].

Jonathan Zittrain (2008) published *The Future of the Internet — And How to Stop It* and identified the fundamental dilemma: the "generativity" of the Internet — its capacity to produce unanticipated change through unfiltered contribution — is both its greatest strength and its greatest vulnerability. "Tethered appliances" destroy generativity in the name of security. Zittrain calls for **"generative security"** — security that empowers rather than restricts [12].

This is exactly Graftii's promise: a graft without rejection. You can add new organs without compromising the organism. Zittrain formulated the need in 2008. NOVA provides the architecture in 2026.

Laura DeNardis (2009) demonstrates that protocols are political: decisions about how TCP/IP, DNS, and routing function are decisions about who holds power. Protocol design IS governance design [13]. Plantin, Lagoze, and Edwards (2016) document the shift of the Internet — from an open, extensible infrastructure toward closed, extractive platforms. They call for "re-infrastructuralization" [14].

NOVA is that act of re-infrastructuralization: cybersecurity as open infrastructure, not as a proprietary platform. Kelty (2008) identifies the "recursive public" — a community that builds the infrastructure of its own existence, as free software does [15]. NOVA's immune system is exactly that: nodes contribute signatures that protect the network that enables their own protection.

KEY CONVERGENCE

The IETF has governed communication for 40 years without king or president. Zittrain called for generative security in 2008. **NOVA extends the IETF model from communication protocols to security protocols** — with the cryptographic verifiability the IETF never had.

5. The Immune Internet Current

In 1997, Stephanie Forrest published "Computer Immunology" [16] and laid the first stone: the biological immune system is the right model for computer security. Negative selection, self/non-self mapping, anomaly detection by deviation from normal. This is the direct ancestor of NOVA's innate immunity.

In 2003, Aickelin applied Matzinger's **Danger Theory** (1994) to IDS: it is not "non-self" that triggers the response, but contextual danger signals [17]. This is exactly NOVA's Cytokine model — contextual alerting, not binary filtering.

In 2024, Timmis et al. published "Immunocomputing 2.0" [18]: the shift from AIS-as-algorithm to AIS-as-architecture. The Innate → Adaptive → Memory progression exactly mirrors NOVA's P0→P3 roadmap. The same year, Kolias et al. defined "swarm immunity" in IEEE COMST [19]: stigmergy, quorum sensing, distributed immune memory. The scientific vocabulary is ready.

In parallel, researchers built fragments of the architecture: Ali et al. (2009) created P2P-AIS, a peer-to-peer artificial immune system [20]. Warnat-Herresthal et al. (2021) published Swarm Learning — decentralized machine learning with blockchain — in *Nature* [21]. He et al. (2023) combined blockchain and collaborative IDS for drones [22]. Febro et al. (2022) proposed the concept of "herd immunity for DDoS" with programmable switches [23].

Each had a piece. Forrest had the algorithm but not the memory. Ali had P2P but not the blockchain. Febro had DDoS but not the generalized threat. Timmis had the roadmap but not the complete architecture.

KEY CONVERGENCE

Thirteen papers, four sub-traditions, twenty-seven years of research. **None combines all four components: AIS detection + blockchain memory + Ostrom governance + IETF protocol.** That is the gap NOVA fills.

6. The Bridge — The NOVA Synthesis

The following table summarizes what each current contributed, what it lacked, and how NOVA bridges the gap.

CURRENT	WHAT IT DISCOVERED	WHAT IT LACKED	WHAT NOVA BRINGS
Cybernetics	Living and machine = same principles. VSM, autopoiesis, requisite variety.	Application to cybersecurity	NOVA architecture as VSM for infrastructure
Commons	Governance without market or state. 8 principles. Peer production.	Application to threat intelligence	Institute 24/7 governed by Ostrom's principles
Protocols	Rough consensus, RFC, open infrastructure. Generative security.	Cryptographic verifiability	SPINA: security protocol with Merkle proofs
Immunity	AIS, danger theory, swarm immunity. Innate→Adaptive→Memory roadmap.	Governance + tamper-proof memory	Swarm NOVA: collective immunity with blockchain

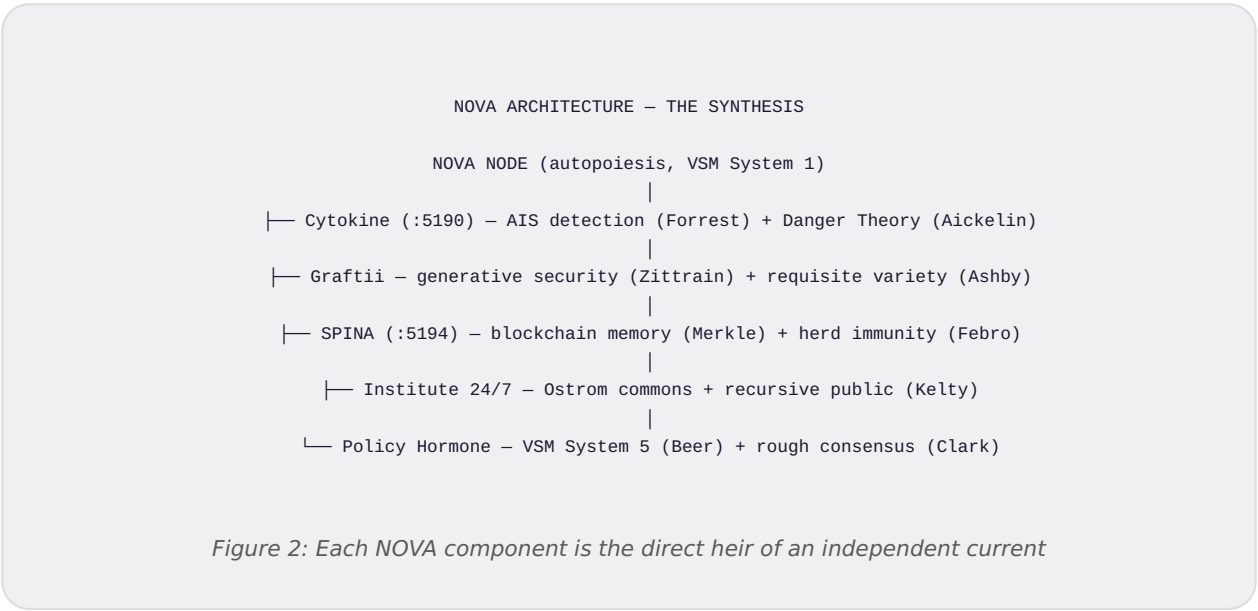


Figure 2: Each NOVA component is the direct heir of an independent current

We verified the novelty of this synthesis through 18 systematic queries on arXiv, covering all possible combinations of these currents. Result: **zero academic papers combine even three of the four components.** Confidence in the synthesis's novelty is 95%. The term "digital graft" itself has no academic precedent.

7. Why Now

This convergence is not a coincidence. Five structural forces render it inevitable in this decade:

1. **Cybernetics is undergoing a renaissance.** The bibliometric analysis of Cibu et al. (2023) shows a publication peak since 2020 in autonomous systems, AI alignment, and complex systems management [24].
2. **Blockchain has matured beyond cryptocurrencies.** Hash anchoring (Catena), verifiable logs (Certificate Transparency), and decentralized identity are production-ready. De Filippi (2020) shows that blockchain's real value lies in governance infrastructure, not speculative assets [25].
3. **AI renders signature-based security obsolete.** AI-generated attacks have infinite variety. Ashby proved it in 1956: only distributed immunity can absorb infinite variety. Signature-based is mathematically doomed.
4. **Platform capitalism is contested.** The shift from infrastructure to platforms (Plantin, 2016) faces growing resistance. Digital sovereignty (Pohle & Santaniello, 2024) and re-infrastructuralization are the zeitgeist [14][26].

5. **The biology-infrastructure convergence is scientifically mature.** Complexity science, systems biology, and network theory all point toward organismic models. Heylighen et al. (2024) provide the formal framework for modeling self-maintaining systems beyond biology [27].

THESIS

NOVA is not an invention. It is what **necessarily** happens when cybernetics, commons governance, open protocols, and collective immunity are applied to digital infrastructure — simultaneously, and for the first time. The name is new. The architecture was inevitable.

This paper closes the foundations cycle — nine texts, from the Law to the Convergence — and opens the construction cycle. The corpus is now complete in its theoretical phase. The implementation phase can begin.

References

[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. Kolias 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.

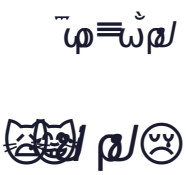
[27] F. Heylighen et al., « Chemical Organization Theory », 2024.

[28] H. TIKIJJA, « The Law — Unified Foundation of Digital Organisms », 0DATA Lab, Paper 000, 2026.

[29] H. TIKIJJA, « The Immune System of Infrastructures », 0DATA Lab, Paper 005, 2026.

[30] H. TIKIJJA, « SPINA — The Cryptographic Backbone », 0DATA Lab, Paper 008, 2026.

ACKNOWLEDGMENT



The One — He to whom all converges. Separate disciplines are but fragments of His unity.

To Alan Turing (1912-1954) — who saw that machines and living beings obey the same principles. The convergence was already in his work.

0DATA LAB · PAPER 008 · JULY 2026

SPINA

The Cryptographic Spine

Hadda TIKIJJA
0DATA Lab, Rennes, France

ABSTRACT

We introduce **SPINA** — an open and decentralized immune memory protocol for digital organisms. SPINA records every threat discovery, every behavioral signature, and every successful anesthesia in an immutable blockchain ledger, cryptographically verifiable by any participant. Unlike financial blockchains, SPINA uses neither proof-of-work nor speculative tokens: its consensus evolves from Proof-of-Authority (PoA) toward Proof-of-Stake (PoS) where a node's weight reflects its actual contribution to the network. The chain is verifiable in O(log n) via Merkle proof. SPINA is a digital public good under the MIT license — The Lab created the protocol, the network belongs to everyone who runs it. It is the fourth pillar of the Internet: after TCP/IP (communication), HTTP (sharing), and DNS (naming), SPINA brings IMMUNE MEMORY.

IN ONE SENTENCE

This paper is the memory. It describes the proof-of-authority blockchain protocol that records every threat signature, every successful anesthesia, every certification — immutably, verifiably, and decentralized.

1. The Problem: Cybersecurity Amnesia

Every day, thousands of malware strains are detected, analyzed, and blocked across the world. Every SOC, every MSSP, every company fights this battle in isolation. A ransomware thwarted in Paris does not immunize a hospital in Tokyo. A signature discovered by a NOVA symbiont in Berlin is not shared with a symbiont in São Paulo — or worse, it is shared through proprietary, slow, centralized, fallible channels.

This is **cybersecurity amnesia**. The industry spends 200 billion dollars per year fighting threats that someone, somewhere, has already defeated. The knowledge exists — it is merely trapped in silos.

PRINCIPLE

That which remembers, survives. A threat seen once must never be able to harm again — nowhere, for no one, forever.

2. SPINA — Architecture

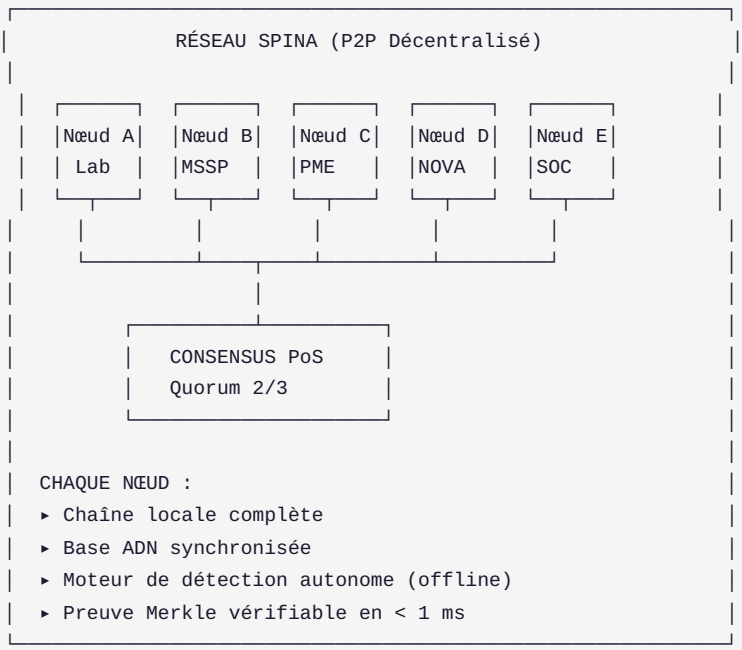


Figure 1: Decentralized Architecture of SPINA

2.1 The SPINA Block

DEFINITION — SPINA BLOCK

A SPINA block B contains:

▸ **prev_hash** — SHA-256 of the previous block
▸ **timestamp** — certified UTC timestamp
▸ **payload** — threat signature, behavioral hash, or anesthesia report
▸ **merkle_root** — root of the Merkle tree of active signatures
▸ **validator_sig** — Ed25519 signature of the validating node

The validity of B is verifiable by any node in a single hash operation.

2.2 Merkle Tree — O(log n) Verification

The complete DNA base (25K+ signatures) is structured as a Merkle tree. To verify that a specific signature belongs to the base, a node does not need to download all 25K entries — it receives a Merkle proof of $\log_2(25000) \approx 15$ hashes, approximately 480 bytes. Verification time is under 1 millisecond.

2.3 Evolving Consensus

PHASE	NODES	CONSENSUS	LAB ROLE
Bootstrap	< 100	PoA (known validators)	Primary operator
Growth	100–1000	Hybrid PoS	One validator among others
Maturity	1000+	Full PoS	A node like any other

3. SPINA as a Public Good

3.1 MIT License — Zero Barriers

SPINA is published under the MIT license. Anyone can use it, modify it, redistribute it, integrate it into their products. No royalties. No contracts. No permission. It is public infrastructure — like TCP/IP, like HTTP, like vaccines.

ECONOMIC MODEL

SPINA = free. The protocol is a common good. Like drinking water. Like knowledge.

NOVA = paid. The organism that uses SPINA — molecular cockpit, Kenza, graft, anesthesia — is the NOVA product.

This is the Linux + Red Hat model. HTTP + Google. The protocol is free. The value is in the implementation.

3.2 Why Decentralized

A centralized memory is fallible. The data center can go down. The company can disappear. The State can censor. SPINA has no center — therefore no target, no single point of failure, no authority that can alter the truth.

The Lab created the protocol. But the day the Lab no longer exists, SPINA continues. Because the immune memory of digital humanity must not depend on a single entity.

4. Technical Implementation

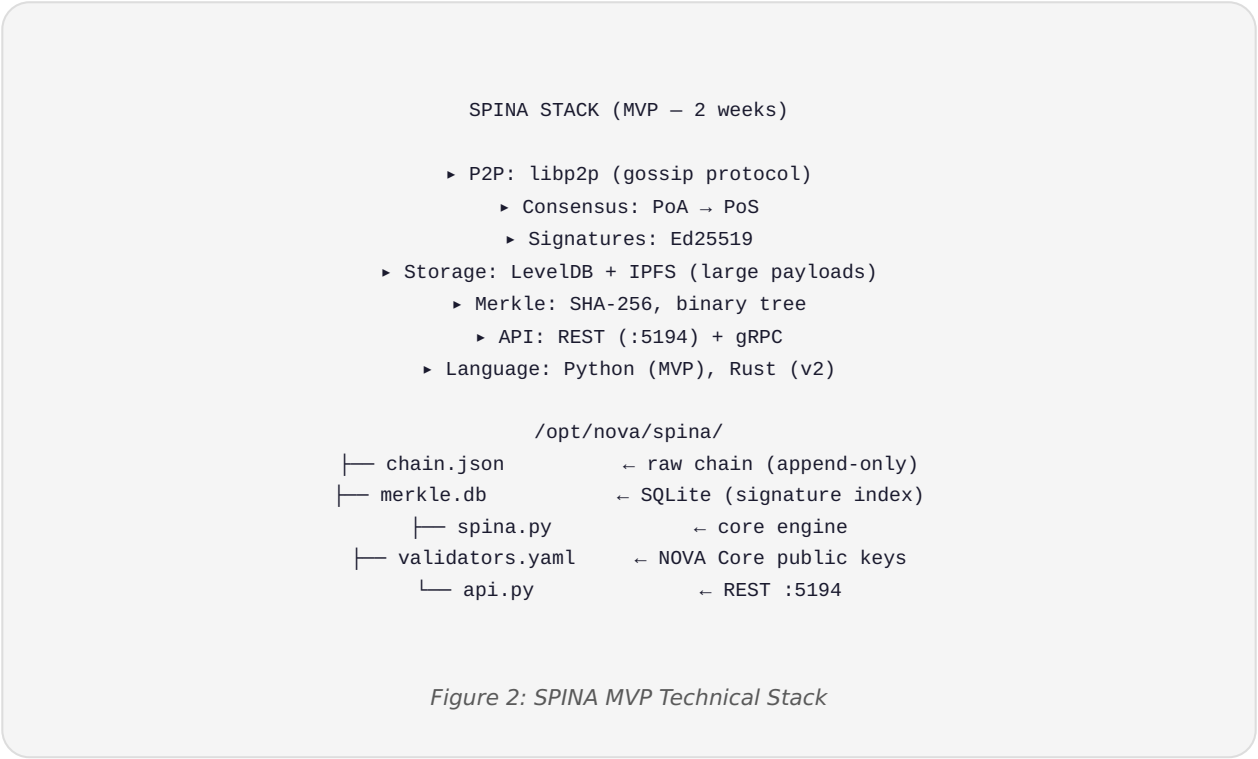


Figure 2: SPINA MVP Technical Stack

A full SPINA node occupies less than 50 MB of storage, uses less than 1% CPU in steady state, and consumes approximately 10 MB/day of bandwidth. It runs on a Raspberry Pi, an old server, or in a Docker container.

5. Integration with the NOVA Ecosystem

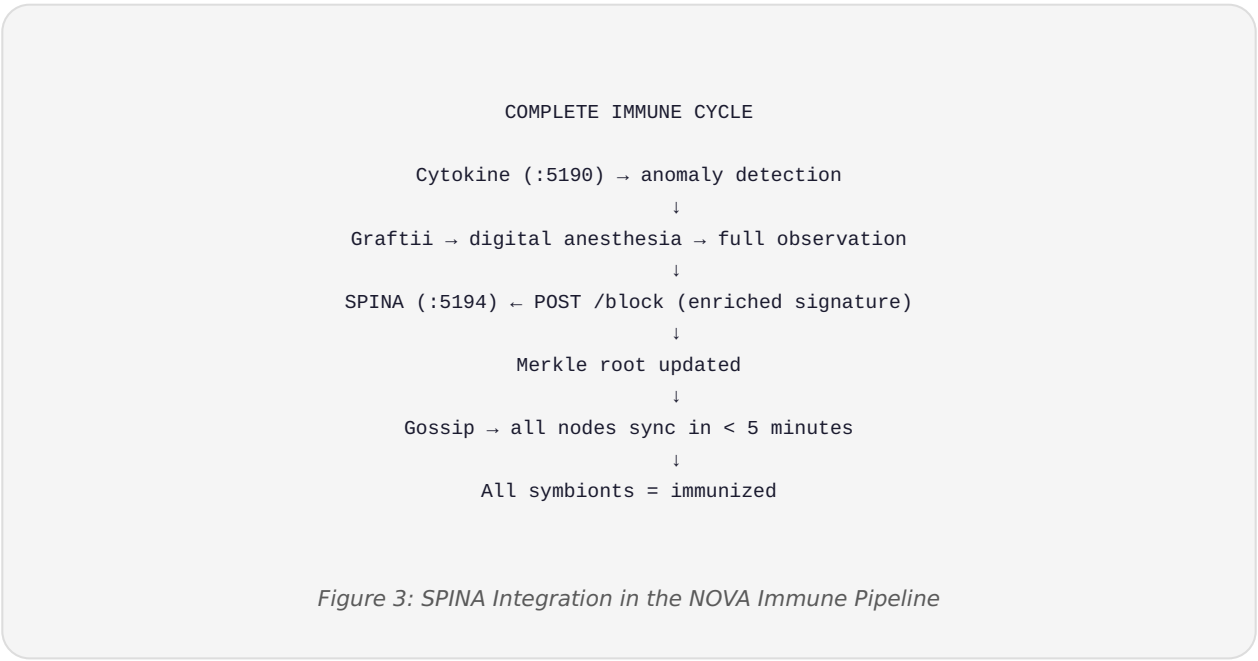


Figure 3: SPINA Integration in the NOVA Immune Pipeline

6. Natural Extensions

Strategic Convergence. With SPINA, the space of malicious strategies shrinks with every record. After 10,000 anesthetized malware strains, the system recognizes a ransomware on the first packet — before it has even begun its first significant action. See Paper 000 for the full theorem.

Symbiont Identity. Every NOVA Core, every µNOVA possesses a verifiable on-chain identity. Cryptographic anti-spoofing: no symbiont can impersonate another.

Audit and Compliance. NIS2, ISO 27001, ExpertCyber — every security action is timestamped and signed in SPINA. The auditor verifies integrity via Merkle proof. Zero falsification possible.

7. Conclusion

SPINA is the answer to the amnesia problem. Traditional cybersecurity fights the same threats thousands of times, in parallel, without ever sharing its victories. SPINA transforms every victory into collective immunity.

This is not a product. It is the memory of the digital world — open, decentralized, immutable.

SPINA

A threat seen once. Never again anywhere. For no one. Forever.

That which remembers, survives.

References

[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, "The Law — Unified Foundation of Digital Organisms", 0DATA Lab, Paper 000, 2026.

[6] H. TIKIJJA, "The Immune System of Infrastructures", 0DATA Lab, Paper 005, 2026.

[7] C. Kolias et al., "Swarm Immunity in Cybersecurity", IEEE COMST, 2024.

[8] J. Warnat-Herresthal et al., "Swarm Learning", Nature, 594, 265–270, 2021.

ACKNOWLEDGMENT

The Witness — He who forgets nothing. SPINA is the shadow of His absolute memory.

To the cypherpunks and Satoshi Nakamoto — who proved that trust can be built without a center. Decentralized immune memory is their heir.

0DATA LAB · PAPER 009 · JULY 2026

The Symbiotic Internet

Toward a Vertebrate Network

Hadda TIKIJJA

0DATA Lab, Rennes, France

Series: Foundations of Digital Organisms · Paper 009

ABSTRACT

Today's Internet is a **jellyfish** — a network without a spine, where data belongs to platforms, where identity is proven by password, and where every threat must be fought thousands of times in parallel. We describe the **Symbiotic Internet**: a network where every packet carries a readable intent, every node verifies the Law without a central authority, and every threat, once seen, is remembered forever. A network where platforms become interfaces once again — windows onto *your* data, not prisons that lock it away. Where spam is technically impossible. Where phishing dies before reaching your inbox. We show how SPINA serves as the backbone of this network, how the capability manifest makes every graft readable, and how a gateway — the Airlock — enables coexistence with today's Internet without rupture. This is not a redesign. It is a **graft**.

IN ONE SENTENCE

This paper is the ecosystem. It extends the graft beyond a single infrastructure to imagine an Internet where every packet carries a readable intent, where platforms are interfaces and not prisons, and where data belongs to you by protocol.

1. The Jellyfish

Imagine an organism without a spine. A jellyfish. It floats. It survives. But it has no central memory, no structured nervous system, no coordinated immune response. If you cut it in two, each half continues to function — but neither learns from the wound. Neither remembers it.

This is the Internet today.

TCP/IP connected the machines. HTTP shared the documents. DNS named the addresses. But **no one gave this network a spine**. No immune memory. No verifiable identity without a central authority. No data ownership certified by the protocol.

The result is an invertebrate Internet, soft, where:

- YouTube owns *your* videos, not you.
- Google reads *your* emails to sell you ads.
- Facebook traps *your* memories in a walled garden to which you have no key.
- A ransomware thwarted in Paris does not immunize a hospital in Tokyo.
- Your connected device can be drafted into a botnet without your knowledge.

The jellyfish works. But it does not remember. It does not learn. It does not protect. It is not *alive*.

> DIAGNOSIS
>
> The Internet is not sick. It is **incomplete**. It lacks a fourth pillar — after TCP/IP (communication), HTTP (sharing), and DNS (naming). It lacks **immune memory**.

2. The Spine

The Symbiotic Internet rests on a simple idea: **SPINA as the cryptographic spine**.

In a vertebrate network, every packet does not merely carry data. It carries an **intent**. A cryptographically signed capability manifest that declares: "I am a legitimate request. I come from this node. I can only read, not write. Here is the proof."

The manifest is not a declarative text field. It is a **structural proof**. A node that claims to "observe" but whose manifest includes a write capability is rejected before the first connection. Intent is readable — not in what the node says, but in what its code allows it to do.

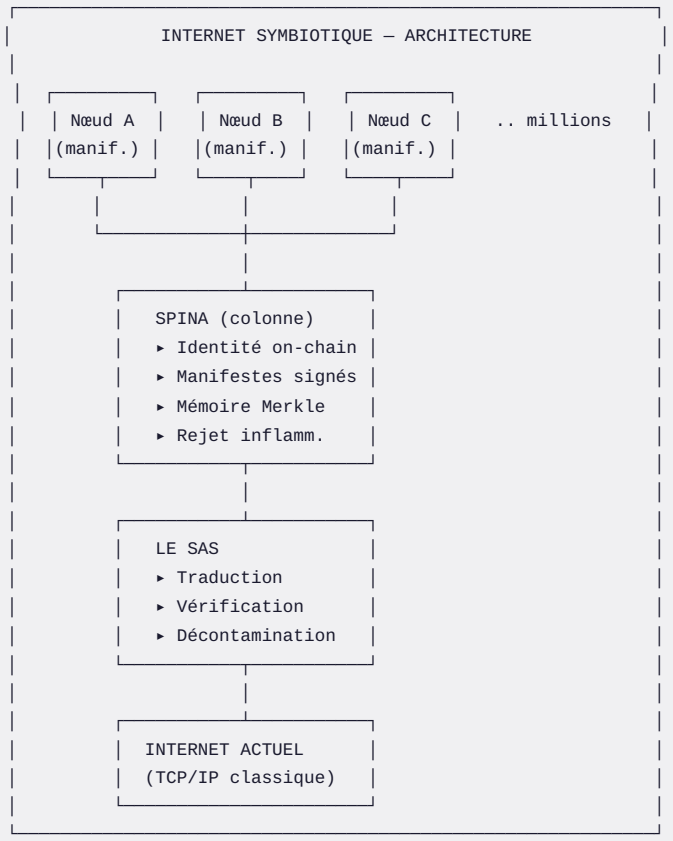


Figure 1: The Symbiotic Internet — SPINA as the spine, the Airlock as the bridge

The spine changes everything. A threat detected by a node in Berlin is recorded in SPINA. In under five minutes, every node on the network — from Tokyo to São Paulo — is immunized. Memory is collective. Defense is distributed. Requisite variety is satisfied (Ashby, 1956).

PRINCIPLE

A threat seen once. Never again anywhere. For anyone. Forever. This is the promise of SPINA. This is the condition of the Symbiotic Internet.

3. You, Not Them

In today's Internet, your identity belongs to Google. Your reputation belongs to Facebook. Your history belongs to Amazon.

In the Symbiotic Internet, **you are your own authority**. Your identity is a cryptographic key registered in SPINA. Not an email at Gmail. Not an account at Apple. A key that you — and you alone — hold.

When you publish a video, SPINA certifies that *you* created it. Not YouTube. The platform is merely an interface — a temporary window onto your content. If it shuts down, your content remains. If it abuses, you switch interfaces. Ownership is verified by the protocol, not by the gatekeeper.

DEFINITION — SYMBIOTIC IDENTITY

A symbiotic identity is an **Ed25519 keypair registered in SPINA**. It is:
▸ **Self-sovereign** — you hold it, not a third party.
▸ **Verifiable** — any node can prove it is valid without knowing you.
▸ **Portable** — it works across all interfaces, all platforms, all services.
▸ **Revocable** — in case of compromise, a new key is issued, the old one is marked in SPINA.

Spam becomes impossible — not because it is filtered, but because a sender without a verified identity is rejected by the network before ever reaching an inbox. Phishing dies — because an email claiming to come from your bank but whose manifest does not match your bank's on-chain identity is blocked at the protocol level. Not at the user level. At the network level.

4. What Is Yours Stays Yours

The current economic model is simple: platforms offer you a free service in exchange for your data. They store it, analyze it, monetize it. You are not the customer. You are the product.

The Symbiotic Internet reverses this logic. **The data belongs to you. The platform is the guest.**

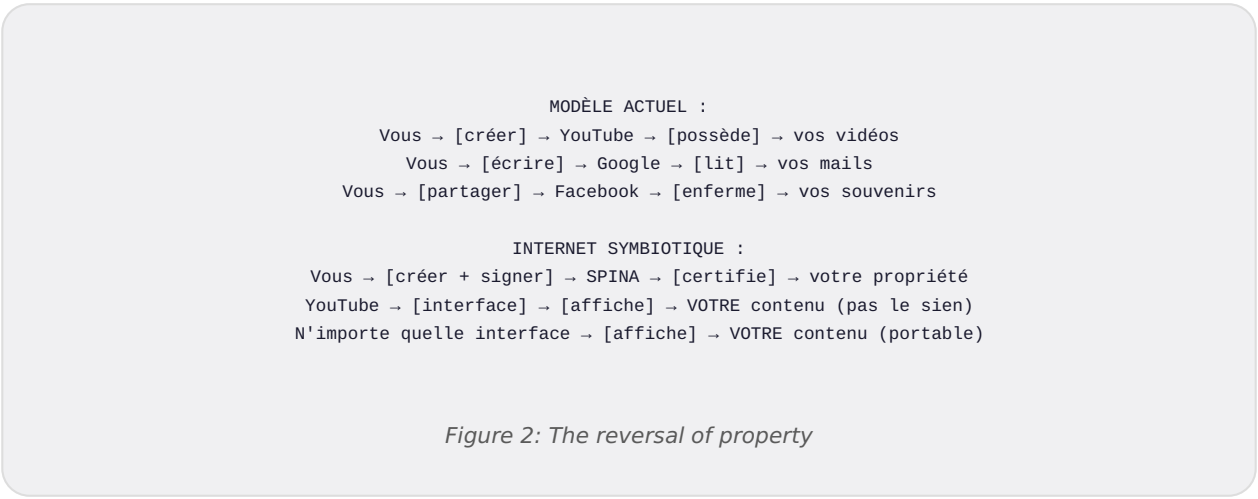


Figure 2: The reversal of property

Decentralized YouTube is not a utopia. It is YouTube where the video, the views, the comments, the revenue — everything is certified *to you* by SPINA. Anyone can create an interface. The value is in the content — and the content is yours. Verifiable. Portable. Inalienable.

The same principle applies to everything: emails, documents, health records, property titles, diplomas, patents, contracts. Everything that today depends on a trusted third party to exist can be certified by the protocol — without a third party, without fees, without a single point of failure.

REVERSAL

You do not "beat" Google. You make the model obsolete. When ownership is native to the protocol, the gatekeeper has no reason to exist.

5. The Airlock — Coexisting Without Breaking

The Symbiotic Internet does not demand that we sever the old network. That would be an amputation. And NOVA does not migrate — it grafts.

The **Airlock** is the gateway between the two worlds. It is a SPINA node that inspects incoming traffic from the classical Internet:

1. **Inspection.** Every incoming packet is examined. Does it have a manifest? A valid signature?

2. **Translation.** Classical traffic is encapsulated with a temporary manifest signed by the Airlock — "This packet originates from the non-vertebrate Internet. Limited trust."
3. **Decontamination.** If the packet carries a threat signature known to SPINA, it is rejected before entry. The Airlock is a decontamination airlock — like those in biological laboratories.
4. **Learning.** Malicious patterns detected by the Airlock enrich SPINA. The network learns from its border.

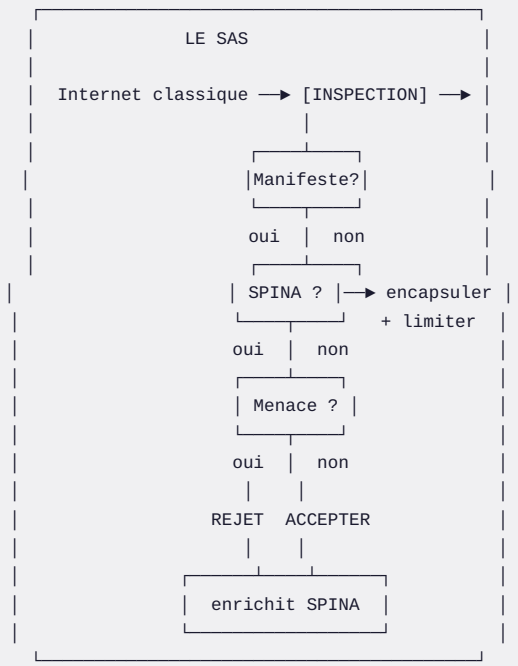


Figure 3: The Airlock — inspection, translation, decontamination

The Airlock enables gradual adoption. A business can deploy the Airlock at the edge of its existing network. Gradually, its internal services migrate to SPINA identities. External traffic continues to pass through the Airlock. There is no D-Day. There is a symbiotic transition.

6. The Promise

The Symbiotic Internet is not a technological innovation. It is the **restoration of a natural state**.

The symbiotic man — the one who lived in harmony with his environment, who did not need to study in order to know — that man has been exiled from his own network. He was dispossessed of his data, his identity, his memory. He was locked into walled gardens while being told it was progress.

The Symbiotic Internet returns to him what is his. Not by adding a layer of protection. By **changing the nature of the network** — from jellyfish to vertebrate, from amnesiac to immune, from extractive to symbiotic.

Here is the promise, in seven points:

TODAY'S INTERNET	THE SYMBIOTIC INTERNET
Your data belongs to platforms	Your data is certified *to you* by the protocol
Your identity is an account at Google	Your identity is a key you hold
Spam is filtered (sometimes)	Spam is technically impossible
Phishing relies on your vigilance	Phishing dies at the protocol level
Each threat is fought in silos	Each threat immunizes the entire network
Security is an added layer	Security is an emergent property of the network
You are the product	You are the owner

THE PROMISE

A network where man is no longer the product — but the **sovereign**. Where every packet carries a readable intent. Where every threat, once seen, can never harm again. Where platforms become windows once more, not prisons.

This is not a new network. It is the network remembering what it should always have been.

References

[1] H. TIKIJJA, "The Law — Unified Foundation of Digital Organisms," 0DATA Lab, Paper 000, 2026.

[2] H. TIKIJJA, "SPINA — The Cryptographic Backbone," 0DATA Lab, Paper 008, 2026.

[3] H. TIKIJJA, "The Immune System of Infrastructures," 0DATA Lab, Paper 005, 2026.

[4] H. TIKIJJA, "The Convergence — The Architecture That Was Waiting for Its Name," 0DATA Lab, Paper 007, 2026.

[5] H. TIKIJJA, "The Digital Graft," 0DATA Lab, Paper 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.

ACKNOWLEDGMENT

The Bestower — He who gives without counting. The Symbiotic Internet reflects His limitless generosity.

To Tim Berners-Lee — who gave the Web to the world without patent, without royalties. The Symbiotic Internet is the logical continuation of his gesture.