Digital Infrastructure Alliance

A Multinational Framework for Open Source Sustainability

December 2025

Executive Summary

Open source software underpins global digital infrastructure, contributing an estimated $8.8 trillion to the world economy and €65-95 billion annually to the EU alone. Yet this critical foundation remains chronically underfunded, maintained largely by unpaid volunteers vulnerable to burnout, abandonment, or—as the xz Utils incident demonstrated—social engineering attacks.

Current funding mechanisms are fragmented: individual government programs operate in isolation, corporate sponsorship remains inconsistent, and the EU's Next Generation Internet program faces elimination despite supporting 500+ projects. Meanwhile, European governments collectively spend billions on proprietary software licenses while the open infrastructure underlying their digital economies receives scattered, inadequate support.

This brief proposes a **Digital Infrastructure Alliance**—a treaty-based multinational framework modeled on established collaborative institutions (NATO, ESA, CERN) that pools resources from participating democracies to sustainably fund critical open source components. Initial projections suggest 10-15 founding members could generate €300+ million annually in coordinated funding, representing a transformational increase in organized support while reducing per-member costs through burden sharing.

The timing is critical. EU budget negotiations for 2028-2034 are underway. Germany's Sovereign Tech Fund has proven the model viable. Geopolitical pressures around digital sovereignty are intensifying. The infrastructure exists; what's needed is coordination.

I. The Infrastructure Crisis

The Paradox of Value and Investment

Ninety-six percent of all codebases contain open source components. The Linux kernel runs supercomputers, smartphones, critical infrastructure, and the majority of web servers. LibreSSL and OpenSSL secure internet communications. Systemd manages service initialization across millions of systems. These aren't niche tools—they're foundational infrastructure.

Yet many critical projects operate on a fraction of what would be considered minimal sustainable funding. The xz Utils backdoor attempt in early 2024 highlighted how a single overworked maintainer became the target of a sophisticated social engineering campaign precisely because the project lacked resources for proper security review and maintainer support. The attack vector wasn't technical sophistication; it was exploiting the chronic under-resourcing of essential infrastructure.

Consider the asymmetry: a ransomware attack leveraging a vulnerability in widely-deployed open source software can cost billions in economic damage. The annual budget to maintain that software? Often less

than a mid-sized company's coffee budget. This isn't sustainable, and the costs of failure are systemic rather than localized.

Current Funding Landscape: Fragmented and Insufficient

Government Programs:

Germany's Sovereign Tech Fund represents the current state of the art—€23 million invested across 60+ projects in its first two years, with 500 applications requesting €114 million in total. This demonstrates both the viability of public funding and the massive unmet demand. However, the STF operates as a single-nation initiative with inherent scaling limitations.

The EU's Next Generation Internet program provided €27 million supporting 500+ projects through cascade funding mechanisms. Despite proven effectiveness and low bureaucracy, NGI has been eliminated from the draft 2025 Horizon Europe budget, replaced by a €10 million "Open Europe Stack" program—a 63% funding cut at precisely the moment when digital sovereignty concerns should be driving increased investment.

Corporate Sponsorship:

While companies like Microsoft, Google, and Amazon contribute to open source through foundations and direct project funding, this support remains strategically inconsistent, subject to quarterly earnings pressures, and concentrated on projects that serve immediate corporate interests rather than broader infrastructure needs. The Linux Foundation's annual budget of approximately €177 million, while significant, relies heavily on corporate members whose priorities may not align with long-term commons sustainability.

Individual Donations:

Platforms like GitHub Sponsors, Open Collective, and Patreon enable direct support for maintainers, but the model scales poorly. High-profile projects may receive adequate funding while equally critical but less visible infrastructure languishes. The model also places maintainers in the uncomfortable position of constantly marketing for survival rather than focusing on technical work.

The Free-Rider Problem at Scale

Every entity using open source software benefits; few contribute proportionally to the value extracted. A government agency running thousands of Linux systems, a corporation building products on open frameworks, a university conducting research with open tools—all extract enormous value while maintenance costs are externalized to volunteer labor or scattered, inadequate funding.

This isn't a moral failing but a structural problem requiring structural solutions. Individual rationality (why should I pay when others don't?) produces collective irrationality (critical infrastructure maintained by burned-out volunteers). The solution lies not in appeals to altruism but in coordinated institutional frameworks that align incentives and distribute costs equitably.

II. The Case for Multinational Coordination

Why National Programs Aren't Sufficient

Germany's Sovereign Tech Fund demonstrates that government funding for open source infrastructure can work. The program operates with low bureaucracy, makes strategic investments in foundational technologies, and has created a model other nations are studying. However, scaling through replication—each country launching its own STF—introduces inefficiencies:

Fragmentation of Effort:

Maintainers face the burden of applying to multiple national programs, each with different criteria, timelines, and reporting requirements. A critical library serving users in ten countries shouldn't require ten separate funding applications. The administrative overhead defeats the purpose of making maintainers' lives sustainable.

Duplication and Gaps:

Without coordination, countries may fund overlapping priorities while leaving other critical areas unsupported. National strategic interests don't perfectly map to global infrastructure needs. A library essential to European automotive systems, Japanese robotics, and Canadian telecommunications requires coordinated rather than siloed investment.

Reduced Leverage:

Ten countries each investing €20 million independently generate €200 million in funding but with fractured priorities and duplicated administration. The same €200 million pooled strategically, with coordinated governance and unified application processes, provides far greater impact per euro spent.

Political Vulnerability:

Single-nation programs remain vulnerable to budget cuts, political transitions, or shifting priorities. Germany's coalition government changes could affect STF funding. A multinational treaty framework provides institutional stability that transcends individual election cycles.

The NATO Burden-Sharing Model

NATO's collective defense framework offers a proven template for multinational cooperation with analogous characteristics:

Shared Threat, Shared Investment:

In NATO, an attack on one member threatens all; collective defense serves mutual interests. In digital infrastructure, a vulnerability in widely-deployed software affects all users regardless of borders. The xz Utils backdoor didn't respect national boundaries. Supply chain security is inherently collective.

Proportional Contributions:

NATO members contribute based on GDP, ensuring burden sharing reflects economic capacity rather than imposing uniform costs. Smaller economies aren't overwhelmed; larger economies carry appropriate weight. The same model applies naturally to open source funding—contributions scale with economic benefit derived.

Unified Command, Distributed Benefit:

NATO maintains unified command structures while defending all member territories. A Digital

Infrastructure Alliance would pool funding through unified governance while ensuring all participants benefit from improved infrastructure security and sustainability.

Institutional Resilience:

NATO has survived seven decades, multiple political transitions across member states, and evolving threat landscapes precisely because it operates as a treaty-based framework with shared governance rather than depending on any single nation's political will. Open source infrastructure funding requires similar institutional durability.

Precedent: Existing Collaborative Frameworks

European Space Agency (ESA):

Twenty-two member states pool resources for space research and development. Contributing nations gain access to capabilities no single member could sustain independently. Governance balances national interests with collective objectives. The model works for decades-long projects requiring sustained investment.

CERN:

The European Organization for Nuclear Research operates through international treaty, pooling scientific resources from 23 member states (plus observers) to build and operate particle physics infrastructure. Decisions balance national contributions with collective scientific priorities. Non-European states participate as observers, demonstrating the model's extensibility.

International Maritime Organization:

A UN specialized agency with 175 member states coordinating maritime safety, security, and environmental standards. Different contribution tiers allow broad participation while maintaining governance effectiveness. Technical committees ensure decisions remain grounded in domain expertise rather than pure politics.

The common thread: treaty-based frameworks with:

- Pooled financial resources
- Governance balancing national interests and collective objectives
- Technical advisory structures ensuring domain expertise informs decisions
- Institutional continuity transcending political cycles
- Demonstrated multi-decade sustainability

These aren't theoretical models. They work. The question isn't whether multinational coordination can succeed—it's whether the political will exists to apply proven frameworks to digital infrastructure.

III. Proposed Framework: Digital Infrastructure Alliance

Core Principles

1. Burden Sharing Through Proportional Contribution

Member states contribute annually based on GDP, ensuring equitable distribution of costs relative to economic capacity and benefit derived. A provisional formula:

- Minimum contribution: €5 million annually (enables small-economy participation)
- Scaled contribution: 0.001% of GDP for economies above €500 billion GDP
- Voluntary additional contributions welcomed

This generates substantial aggregate funding while keeping per-member costs manageable. Ten founding members (Germany, France, Netherlands, Italy, Canada, Japan, South Korea, UK, Switzerland, Norway) would contribute approximately €200-300 million annually based on current GDP figures.

2. Political Independence, Technical Governance

Funding decisions must be driven by technical merit and infrastructure criticality, not political expedience or national favoritism. The governance structure separates strategic oversight (political) from technical assessment (expert):

Governing Council: Representatives from member states (one vote per country, weighted by contribution tier to prevent free-rider dominance). Sets strategic priorities, approves annual budgets, reviews program effectiveness. Requires 2/3 majority for major decisions.

Technical Advisory Board: Security researchers, senior maintainers, infrastructure experts appointed for staggered multi-year terms. Makes funding recommendations based on criticality assessments, supply chain analysis, and maintainer capacity evaluations. No voting power—advisory only, ensuring technical competence without political capture.

Operational Staff: Professional program managers handling application review, maintainer onboarding, progress monitoring, and reporting. Based on Germany's Sovereign Tech Agency model: lightweight processes, flexible deliverable formats, emphasis on outcomes over bureaucracy.

3. Transparency and Accountability

All funding decisions, governance proceedings, and impact assessments published openly. Regular independent audits verify proper use of funds. Sunset reviews every seven years coinciding with budget cycles, ensuring continued relevance and effectiveness.

4. Global Participation, Democratic Governance

While initially European-focused given EU budget negotiations and existing STF precedent, the framework explicitly welcomes participation from any democratic nation committed to open source sustainability. Non-European democracies (Canada, Japan, South Korea, Australia, New Zealand) face identical digital infrastructure dependencies and would benefit from coordinated investment.

Governance mechanisms prevent any single bloc from dominating while ensuring decisions reflect contributor interests. Advisory observer status available for nations considering membership, facilitating gradual expansion.

Funding Priorities and Mechanisms

Tier 1: Critical Infrastructure Maintenance (50% of budget)

Direct support for widely-deployed foundational components identified through supply chain analysis:

- Core operating system components (kernel, systemd, critical libraries)
- Cryptographic infrastructure (OpenSSL, LibreSSL, GPG)
- Programming language toolchains and package managers
- Web infrastructure (DNS, HTTP servers, content delivery)

Funding targets: €50,000-500,000 per project annually, sufficient to hire full-time maintainers, conduct security audits, improve documentation, and build sustainable community structures.

Tier 2: Ecosystem Strengthening (30% of budget)

Investments improving overall ecosystem health rather than individual projects:

- Security audit programs (proactive vulnerability assessment)
- Accessibility compliance initiatives
- Internationalization and localization support
- Developer tooling and testing infrastructure
- Documentation and onboarding resources

Tier 3: Strategic Gap Filling (15% of budget)

Targeted development addressing areas where proprietary software dominates but open alternatives would serve public interest:

- Professional-grade creative tools (CAD, design, video editing)
- Scientific and engineering software
- Government-specific applications
- Interoperability layers and data portability tools

Tier 4: Emergency Response (5% of budget)

Rapid response fund for:

- Zero-day vulnerabilities requiring immediate remediation
- Critical maintainer burnout (emergency support for abandoned projects)
- Supply chain compromise response
- Coordinated disclosure and patch development

Application and Selection Process

Learning from Germany's STF and addressing NGI's strengths:

Low-Barrier Applications:

Streamlined submission through web portal. Questions designed to assess project criticality, maintainer capacity, and proposed work scope. No extensive grant-writing expertise required. Applications accepted in English and major European languages.

Rolling Assessment:

Quarterly application windows rather than annual cycles, enabling faster response to emerging needs. Initial screening by operational staff, detailed technical assessment by advisory board, final approval by governing council.

Flexible Deliverables:

Progress reporting emphasizes actual work completed (commits, releases, security improvements) over bureaucratic documentation. Accept GitHub repository links, release notes, and brief progress summaries. Annual review calls rather than extensive written reports.

Multi-Year Commitments:

Where appropriate, fund critical projects on 2-3 year cycles rather than requiring annual reapplication. Reduces administrative burden for both maintainers and alliance staff.

Community Input:

Formal mechanisms for community feedback on funded projects and ecosystem priorities. Regular consultations with major distributions, user groups, and security research communities.

IV. Economic and Strategic Rationale

Return on Investment: The Licensing Offset

European governments collectively spend billions annually on proprietary software licenses. Schleswig-Holstein's migration of 30,000 workstations to Linux saves €18 million per year in licensing costs alone—excluding reduced IT support overhead, extended hardware lifecycles, and improved security postures.

Extrapolated conservatively across EU member states:

- ~50 million government workstations across EU
- Average proprietary licensing cost: €200-400 per seat annually
- Total annual licensing expenditure: €10-20 billion

A Digital Infrastructure Alliance investing €300 million annually represents **1.5-3% of current proprietary licensing costs** while funding the infrastructure that enables migration away from vendor lock-in. The ROI becomes positive within years as governments achieve licensing savings exceeding alliance contributions.

This doesn't account for additional benefits:

- Extended hardware lifecycles (Linux runs efficiently on older machines)
- Reduced malware/security incident costs
- Elimination of forced upgrade cycles
- Improved procurement leverage (competitive alternatives reduce vendor pricing power)

Digital Sovereignty: Strategic Independence

The Draghi Report (September 2024) warned that "the EU relies on foreign countries for over 80% of digital products, services, infrastructure and intellectual property." This dependency creates strategic vulnerabilities:

Policy Leverage:

Foreign software vendors can influence policy through access control. If critical government functions depend on proprietary platforms, the threat of service interruption or pricing changes becomes implicit leverage. Open source infrastructure under democratic governance eliminates this vector.

Supply Chain Security:

Closed-source software requires trusting vendors' security practices and access controls. Following NSA revelations and ongoing geopolitical tensions, this trust is increasingly untenable for sensitive government operations. Open source enables direct security audits and verification.

Economic Resilience:

Reliance on foreign tech platforms creates balance-of-payments issues (capital flowing out) and concentrates economic power in non-European entities. Investment in open source infrastructure keeps resources circulating in participating economies while building domestic technical capacity.

Crisis Response:

Geopolitical conflicts, trade disputes, or sanctions can disrupt access to proprietary platforms. Open source infrastructure under multinational democratic governance remains accessible regardless of bilateral political tensions. The software doesn't have a nationality, even if the funding alliance does.

Competitiveness and Innovation

European tech companies compete on an uneven field when their American counterparts benefit from infrastructure effectively subsidized by open source contributions that U.S. corporations dominate. Coordinated public investment levels the playing field:

Reduced Startup Costs:

Open source infrastructure lowers barriers to entry for new companies. Startups can build on mature, well-maintained foundations rather than reinventing basic components or paying license fees that advantage established players.

Standards and Interoperability:

Open standards implemented in open source software prevent platform lock-in and enable ecosystem competition on merit. This contrasts with proprietary platforms using technical lock-in as competitive moat.

Talent Development:

Sustainable funding for open source creates career paths for developers working on infrastructure, retaining technical talent in participating economies rather than seeing it recruited by foreign tech giants.

Technology Transfer:

Government-funded open source development generates knowledge spillovers benefiting broader economies. Unlike proprietary development where learnings remain locked in corporate IP, open source ensures innovations flow freely to all participants.

V. Implementation Roadmap

Phase 1: Foundation (Months 1-6)

Founding Coalition Formation:

Germany (existing STF provides operational model), France (digital sovereignty advocacy), Netherlands (tech-forward government), and 2-3 additional European nations form initial working group. Canada invited as non-EU founding member, establishing precedent for global democratic participation.

Treaty Drafting:

Working group develops foundational treaty establishing:

- Governance structure and voting mechanisms
- Financial contribution formulas and payment schedules
- Technical advisory board composition and appointment
- Operational agency structure and staffing
- Transparency and accountability requirements
- Amendment and expansion procedures

Stakeholder Consultation:

Engage open source community (major foundations, distributions, projects), industry (tech companies dependent on OSS), and civil society (digital rights organizations, transparency advocates) in treaty development. Incorporate feedback while maintaining core principles.

Phase 2: Institutional Setup (Months 7-12)

Treaty Ratification:

Submit to national parliaments in founding member states. Requires legislative approval similar to other international treaty commitments. Target: ratification by minimum 5 members to proceed.

Operational Agency Establishment:

Create administrative entity (potentially housed within existing institution like European Research Area or as standalone agency). Recruit operational staff:

- Executive director and leadership team (3-5 positions)
- Program managers for funding tracks (5-10 positions)
- Technical staff for supply chain analysis and security assessment (3-5 positions)
- Administrative support (2-3 positions)

Total initial staff: 15-25, scaling with program growth.

Technical Advisory Board Appointment:

Member states nominate candidates; selection committee ensures geographic diversity and domain expertise. Initial board: 12-15 members serving staggered 3-year terms to ensure continuity.

Application Infrastructure:

Build or adapt web-based application portal (potentially based on existing grant management systems). Develop assessment criteria, scoring rubrics, and review workflows.

Phase 3: Initial Operations (Year 1)

First Funding Round:

Launch initial calls for proposals across all funding tiers. Conservative initial allocation (€100-150 million) while operational processes mature. Focus on proven critical infrastructure with straightforward assessment criteria.

Process Refinement:

Iterate on application procedures, review mechanisms, and reporting requirements based on initial round feedback. Adjust bureaucratic load and timeline based on maintainer and staff experience.

Impact Assessment Framework:

Establish metrics for measuring program effectiveness:

- Security vulnerabilities identified and remediated
- Maintainer sustainability indicators (bus factor, burnout risk)
- Ecosystem health metrics (contribution patterns, project vitality)
- Economic impact (licensing savings, innovation metrics)

Phase 4: Expansion and Maturation (Years 2-3)

Additional Members:

Recruit additional European nations and expand to interested democracies globally (Japan, South Korea, Australia, potentially others). Each addition brings new funding and broadens governance representation.

Full-Scale Operations:

Ramp to full budgeted capacity (€200-300+ million annually). Expand staff as needed to manage increased application volume. Launch multi-year funding for proven critical projects.

Coordination with National Programs:

Establish formal coordination mechanisms with national-level programs (Germany's STF, any new initiatives in other countries). Avoid duplication while leveraging complementary funding sources.

Industry Partnership:

Create framework for corporate co-funding or matching programs. Industry benefits from improved infrastructure; formalize contributions to supplement public funding without creating governance conflicts.

Phase 5: Long-Term Sustainability (Years 4-7)

First Sunset Review:

Comprehensive program evaluation at 5-year mark. Independent assessment of effectiveness, cost efficiency, and relevance. Inform treaty renewal and structural adjustments.

Integration with EU Budget Cycles:

For EU members, coordinate alliance funding with 2028-2034 and subsequent MFF cycles. Potentially integrate portions of funding through EU budget while maintaining broader multinational structure.

Model Expansion:

Document lessons learned, refine best practices, publish playbooks for other collaborative frameworks. Potential application to other digital commons (data sets, research tools, civic infrastructure).

VI. Addressing Potential Objections

"This Is Just Another Bureaucracy"

The proposal learns explicitly from both successes (Germany's STF, NGI's low-barrier approach) and failures (bloated grant programs with excessive overhead). Key anti-bureaucracy features:

- Streamlined applications (web form, not 50-page proposals)
- Flexible progress reporting (repository links acceptable)
- Technical governance (expert assessment, not political haggling over individual projects)
- Rolling rather than annual cycles (faster response)
- Multi-year funding where appropriate (less churn)

Total administrative overhead target: <10% of budget, comparable to efficient foundations.

"Why Not Just Industry Funding?"

Corporate open source contributions, while valuable, face structural limitations:

Quarterly Pressures:

Public companies optimize for quarterly earnings. Infrastructure maintenance is long-term investment with diffuse rather than concentrated returns. Misalignment between corporate incentives and commons sustainability.

Strategic Capture:

Heavy corporate funding risks projects becoming dependent on sponsors whose interests may diverge from broader community needs. Public funding insulates critical infrastructure from private strategic shifts.

Free Rider Dynamics Persist:

Voluntary corporate contributions don't solve the tragedy of the commons. Companies that contribute subsidize competitors that don't. Public coordination ensures broad cost-sharing.

None of this precludes industry participation—matching programs, direct project support, and foundation contributions remain valuable. Public funding provides baseline sustainability rather than displacing private contributions.

"National Programs Are More Flexible"

National programs offer certain advantages (faster decision-making, alignment with specific national priorities), but multinational coordination provides complementary benefits:

Economies of Scale:

Pooled funding enables larger, more impactful investments in critical infrastructure used globally. A €5 million investment in a widely-deployed library serves all participating nations.

Burden Distribution:

Shared costs enable smaller economies to participate in funding levels they couldn't sustain independently. Luxembourg contributing €5 million to an alliance creates capabilities it couldn't build alone.

Apolitical Technical Assessment:

International governance structures insulate technical decisions from individual nations' political pressures. Harder for any single member to divert funding to pet projects.

The optimal model likely combines both: national programs for country-specific needs and priorities, multinational alliance for foundational infrastructure serving all participants.

"Won't This Just Fund Silicon Valley Projects?"

Governance explicitly addresses geographic and organizational diversity:

Technical Merit, Not Origin:

Funding follows criticality and maintainer need, not project geography. If a U.S.-based project is critical to European infrastructure and underfunded, supporting it serves alliance members' interests.

European Capacity Building:

Strategic gap funding prioritizes areas where European projects exist or could be fostered. Preference for EU-based entities where technical merit is comparable.

Ecosystem Diversity:

Advisory board composition ensures representation from various technical communities, not just largest U.S. foundations. Smaller European projects have voice in priority-setting.

Transparency:

All funding decisions public and justified. Community oversight prevents capture by any single interest bloc.

The goal isn't zero-sum competition with U.S. open source but rather ensuring sustainable infrastructure funding regardless of maintainer location. Infrastructure doesn't have nationality; vulnerabilities don't either.

VII. Windows of Opportunity

EU Budget Negotiations (2025-2026)

The European Commission published its €2 trillion MFF proposal for 2028-2034 in July 2025. Negotiations among European Parliament, Council, and member states are underway now. Budget finalization targets Q2 2026 for January 2028 implementation.

This represents a seven-year budget window—the next opportunity won't come until 2033-2034 negotiations for the 2035+ period. If open source infrastructure funding doesn't achieve meaningful inclusion in the 2028-2034 MFF, the opportunity vanishes for the remainder of the decade.

Current context:

- Next Generation Internet eliminated from current draft (€27 million → €10 million)
- Digital sovereignty rhetoric high but concrete funding uncertain
- Defence spending demands competing for available budget
- Economic pressures limiting overall MFF growth

The risk: digital sovereignty becomes slogan without substance, declaratory policy without funding mechanisms. The opportunity: NGI cuts have created anger in technical community and concern among some policymakers about infrastructure sustainability. A well-articulated alternative framework could redirect that energy productively.

Germany's STF Momentum

Germany's Sovereign Tech Fund has invested €23 million across 60+ projects, received 500 applications totaling €114 million in proposed work, and achieved measurable impact on critical infrastructure security and maintainer sustainability. The 2025 budget increased to €19 million, demonstrating continued political support.

This creates optimal conditions for expansion:

- Proven operational model (don't need to invent from scratch)
- Demonstrable results (not theoretical benefits)
- Experienced staff who understand what works
- Political validation (Bundestag increased funding)

The STF team has explicitly expressed interest in cross-border coordination and European-scale replication. The infrastructure exists; what's needed is the framework to expand scope and pool resources across borders.

Geopolitical Context

Multiple converging factors increase receptivity to arguments about digital infrastructure investment:

U.S. Political Shifts:

The return of volatile U.S. policy creates renewed European interest in strategic autonomy. Trade uncertainty, shifting alliance commitments, and tech platform regulation conflicts all reinforce the case for independent infrastructure.

Security Incident Awareness:

The xz Utils backdoor attempt, SolarWinds compromise, and ongoing supply chain attacks have penetrated policy consciousness. Abstract arguments about "sustainability" become concrete when framed as security imperatives.

Economic Competition:

European Commission focus on competitiveness (Draghi Report, competitiveness fund proposals) creates receptivity to infrastructure investment framed as foundation for innovation and economic strength.

Sovereignty Discourse:

"Digital sovereignty" has moved from activist slogan to official policy priority. The question is no longer whether to pursue it but how. Open source infrastructure funding offers concrete, actionable implementation rather than pure rhetoric.

None of these factors guarantee success, but they create more favorable conditions than existed even 2-3 years ago. The challenge is converting diffuse sentiment into specific policy commitments.

VIII. Call to Action

This framework requires champions—organizations and individuals willing to advocate, refine, and push for implementation. Several specific actions could advance the proposal:

For Open Source Organizations

Open Forum Europe, FSFE, Linux Foundation Europe:

You already engage with EU policymakers and understand Brussels dynamics. This framework provides specific, actionable advocacy asks:

- Champion inclusion of digital infrastructure funding in 2028-2034 MFF negotiations
- Draft model treaty language for multinational coordination
- Coordinate messaging across national advocacy organizations
- Build coalition of supporting organizations and projects

Major Foundations and Projects:

GNOME Foundation, KDE e.V., Apache Software Foundation, Debian, Fedora, Ubuntu—your voices carry weight with both technical community and policymakers. Public statements supporting coordinated multinational funding, sharing maintainer sustainability challenges, and highlighting security implications of underfunding create political pressure.

For Government Relations

Sovereign Tech Agency:

Your operational experience is invaluable. Sharing lessons learned, best practices for low-bureaucracy funding, and challenges of scaling nationally vs. internationally would inform framework design. Potential host or partner for expanded multinational operations.

MEPs and National Representatives:

If you've championed digital policy, open source, or technological sovereignty, this framework offers concrete implementation for abstract commitments. Specific asks:

- Include €200-300 million for open source infrastructure in MFF negotiations
- Support creation of multinational coordination mechanism (even if full treaty takes time)
- Oppose further cuts to existing programs (NGI elimination sets terrible precedent)

For Industry

European Tech Companies:

You depend on open source infrastructure. Public commitments to support coordinated funding (co-funding programs, matching contributions) strengthen the economic case and political viability. Statements to policymakers about competitive implications of U.S./China infrastructure investment create urgency.

Open Source Program Offices:

Corporate OSPOs understand maintainer sustainability challenges firsthand. Participation in technical advisory boards, sharing of supply chain analysis, and advocacy within corporate structures for public funding support all advance the framework.

For Technical Community

Individual Maintainers:

Your voices matter most. Share your experiences—funding challenges, burnout risks, security audit difficulties, the gap between infrastructure criticality and available resources. Personal testimony cuts through policy abstraction.

Distributions and Major Projects:

Formal endorsements of coordinated funding frameworks, participation in consultation processes, and clear articulation of what sustainable funding would enable create specificity that moves policy discussions forward.

For Media and Research

Technical Journalism:

Coverage of these issues shapes both policy attention and community awareness. Investigation of

government licensing costs vs. open source funding, analysis of NGI cuts' implications, and explanatory pieces on why infrastructure funding matters all contribute to informed debate.

Academic Institutions:

Research on open source sustainability, economic impact assessments, case studies of successful funding models (STF, NGI), and policy analysis of digital sovereignty implementation provide evidence base for advocacy and help refine framework design.

IX. Conclusion

The digital infrastructure crisis isn't technical—we know how to write secure, maintainable software. It's institutional. The structures for sustainable funding, coordinated support, and recognition of infrastructure as public good rather than private hobby don't exist at necessary scale.

We have models that work: Germany's STF demonstrates public funding viability, NGI showed low-bureaucracy cascade funding can succeed, NATO proves multinational burden-sharing survives decades. The question isn't whether coordinated infrastructure funding can work but whether political will exists to implement it.

Current conditions create unusual opportunity. EU budget negotiations are live. Digital sovereignty is policy priority rather than fringe concern. Security incidents have demonstrated consequences of infrastructure neglect. Germany's STF provides operational template and experienced team.

What's needed is coordination—converting diffuse support into organized advocacy, translating abstract sovereignty rhetoric into concrete funding commitments, and building multinational framework that transforms €200-300 million in scattered potential funding into focused, sustainable infrastructure investment.

The alternative is continued crisis management: responding to security incidents born of maintainer burnout, watching critical projects languish for lack of €50,000 in support, and seeing billions spent on proprietary licenses while the foundations of digital economies run on volunteer labor.

This brief provides framework. Implementation requires champions willing to advocate, refine, and push through bureaucratic and political obstacles. The infrastructure exists; the need is clear; the window is open. What happens next depends on whether those who understand the stakes are willing to organize around a solution.

Appendices

A. Provisional Budget Model (€300M Annual Alliance)

Category	Allocation	Uses
Critical Infrastructure Maintenance	€150M (50%)	Core OS, crypto, languages, web infrastructure - €50k-500k per project
Ecosystem Strengthening	€90M (30%)	Security audits, accessibility, i18n, documentation, tooling
Strategic Gap Filling	€45M (15%)	Professional tools, government apps, interoperability

Emergency Response	€15M (5%)	Zero-days, maintainer crisis, supply chain incidents
Administration	**<€30M**	Staff (15-25), operations, governance support (<10% overhead)

B. Proposed Founding Members and Contributions

Based on 0.001% GDP for economies >€500B, minimum €5M for smaller economies:

Country	Est. GDP (2024)	Proposed Contribution
Germany	~€4.2T	€42M
France	~€3.0T	€30M
Japan	~€4.0T	€40M
UK	~€3.1T	€31M
Italy	~€2.2T	€22M
Canada	~€2.1T	€21M
South Korea	~€1.8T	€18M
Spain	~€1.6T	€16M
Netherlands	~€1.1T	€11M
Switzerland	~€800B	€8M
Sweden	~€600B	€6M
Poland	~€700B	€7M
Norway	~€500B	€5M
Total (13 members)		**~€257M**

Additional members (Austria, Belgium, Denmark, Finland, Ireland, Australia, etc.) could bring total above €300M. Formula adjustable based on participation.

C. Comparison to Existing Models

Model	Annual Budget	Governance	Scope	Strengths	Limitations
Germany STF	€19M	National	Global projects	Low bureaucracy, proven results	Single-nation vulnerability, scaling limits
EU NGI (cut)	€27M → €10M	EU Commission	EU priorities	Cascade funding, community engagement	Budget instability, EU-only governance
Linux Foundation	~€177M	Corporate members	Global	Large scale, industry connections	Corporate interest alignment, limited public funding
Proposed DIA	€200-300M	Multinational treaty	Global, democratic focus	Burden sharing, institutional stability, coordinated priorities	Requires treaty negotiation, complex governance

D. Key Contacts and Advocacy Targets

(Separate document provided with detailed contact information)

E. Selected References

- GitHub/Open Forum Europe/Fraunhofer ISI, "Feasibility Study: European Sovereign Tech Fund," July 2025
- European Commission, "EU Budget 2028-2034 Proposal," July 2025
- Sovereign Tech Agency, Annual Reports 2023-2024
- Draghi, Mario, "The Future of European Competitiveness," September 2024
- Open Letter on NGI Funding Cuts, July 2024 (500+ signatories)
- Germany Federal Budget 2025, Sovereign Tech Fund allocation
- European Commission, "Open Source Software Strategy 2020-2023"
- OECD, "The Economic and Social Impact of Software," 2021

Document Metadata:

- Version: 1.0
- Date: December 2024
- Status: Draft for community consultation
- Feedback: Welcome and encouraged