OpenForum Europe

Funding Europe's Open Digital Infrastructure

A Study on the Economic, Legal, and Political Feasibility of an EU Sovereign Tech Fund (EU-STF)

By: Nicholas Gates, Jennifer Tridgell, Rosa Maria Torraco, Carsten Schwäbe, Felix Reda, Andreas Hummler, Thomas Streinz, Astor Nummelin Carlberg, and Knut Blind

About OpenForum Europe

OpenForum Europe (OFE) is a not-for-profit, Brussels-based independent think tank which explains the merits of openness in computing to policy makers and communities across Europe.

Originally launched in 2002 to accelerate and broaden the use of Open Source Software (OSS) among businesses, consumers and governments, OFE's focus has since evolved. OFE currently maintains a Policy Research and Development team based in Brussels, which is supported both by our network of partners and supporters, and by specific specialist advisors. The main policy topics that we cover are: Open Source, Open standards, Cybersecurity, Digital Government, Public Procurement, Intellectual Property, Cloud Computing and Internet Policy.

OFE also hosts an independent global network of OpenForum Academy Fellows, each contributing significant innovative thought leadership on core topics, in order to provide new input and insight into the key issues which impact the openness of the ICT market. OFE works closely with the European Commission, the European Parliament, national and local governments, both directly and via its national partners.

OFE aisbl, a Belgian international non-profit association
Transparency number 2702114689-05
Registered in Belgium with enterprise number 721975651
RPM Tribunal de l'Entreprise Francophone de Bruxelles
Registered office: Avenue des Arts 56, 4C, 1000 Brussels, Belgium
Web: openforumeurope.org
e-mail: info@openforumeurope.org

Acknowledgements

This study was led by Nicholas Gates and Astor Nummelin Carlberg from OpenForum Europe with support from our research and writing partners at Fraunhofer ISI and the European University Institute. Those partners included Carsten Schwäbe, Andreas Hummler, and Knut Blind from Fraunhofer ISI and Thomas Streinz, Jennifer Tridgell, and Rosa Maria Torraco from the European University Institute. The study was funded by GitHub and the Digital Infrastructure Insights Fund, and would in particular not have been possible without the generous time, insights, and expertise shared by the GitHub Policy Team, including Felix Reda and Mathias Schindler. It was also shaped immeasurably by the feedback, inputs, and support of the team at the German Sovereign Tech Agency, including Adriana Groh, Paul Sharratt, and Mirko Swillus.

This study was the end product of OFE's longtime engagement over many years with a wide range of stakeholders across Europe and beyond on the need for EU funding for open source sustainability, maintenance, and security, building on the well-established precedent of the German Sovereign Tech Fund. Numerous people's insights have shaped the thinking behind this study, whose names are too numerous to feature here. Additionally, we are deeply grateful to all interviewees and workshop participants who contributed their perspectives to help shape the analysis and recommendations presented in this report. These inputs have been instrumental in shaping the recommendations put forth in this feasibility study, and any remaining errors or omissions are, of course, the responsibility of the authors alone.

In particular, we would like to thank representatives from ENISA, the European Commission (including DG-CNECT), the European Cybersecurity Competence Centre, the European Cyber Security Organisation, the European Parliament, and Germany's Federal Office for Information Security (BSI) for their valuable policy insights. We also extend our thanks to industry leaders and technical experts who offered practical perspectives on the sustainability and security of open source, including representatives from Microsoft, OpenSSF, Acquia, cURL, Siemens, RTE, Mercedes-Benz Group, Mercedes Benz Tech Innovation, Ericsson, and Alliander N.V. Finally, we are indebted to members of the digital funding ecosystem – including the European Artificial Intelligence & Society Fund, the Open Technology Fund, the Prototype Fund, NLnet, the Open Source Technology Improvement Fund – as well as experts from Oxford University and the Stanford Cyber Policy Center, for their thoughtful contributions on the governance, technical, and funding aspects of open digital infrastructure.

Finally, we are grateful to the many others who provided feedback on this study, not least our interview partners but also teams at organisations like Open Future, the Linux Foundation, the Sovereign Tech Fund, and many others. Thank you for your time and efforts in shaping what we hope will be an important contribution.

Foreword by Mercedes-Benz

As vehicles evolve into software-defined platforms, the foundation of innovation increasingly rests on open digital base technologies. These technologies – libraries, frameworks, and tools that underpin critical systems – are not merely components; they are the bedrock of modern software development. At Mercedes-Benz, we recognise that open source software is not a trend but a strategic imperative. It enables collaboration at scale, accelerates innovation, and ensures Europe's technological sovereignty in an era of geopolitical and economic uncertainty.

Today, the European automotive sector faces unprecedented challenges: fragmented standards, dependency on proprietary systems, and the rapid rise of global competitors leveraging open source software ecosystems to disrupt traditional models. Consider software-defined vehicles (SDVs), where functionalities from infotainment to autonomous driving rely on complex software stacks. Proprietary solutions often lock manufacturers into siloed ecosystems, stifling interoperability and inflating costs. Conversely, open source software basic technologies – such as secure communication layers, over-the-air update frameworks, or modular autonomous driving tools – can be shared, improved, and standardised industry-wide. This approach not only reduces redundancy but also democratises innovation, allowing startups and established players alike to build upon a common foundation.

However, it is becoming increasingly apparent that the open source software success story may not be sufficiently sustainable or resilient. While it is positive that there are increasing numbers of commercial consumers of open source software, far too few of these consumers are participating and contributing to the upstream projects, meaning that the vast bulk of the burden of keeping these projects viable and secure falls on unpaid volunteer developers and maintainers. Without sustainable funding and support, it is entirely foreseeable that critical components will degrade, leaving entire industries exposed to systemic risk.

This is why initiatives like the EU Sovereign Tech Fund are so timely. Europe must urgently invest in the open digital infrastructure it relies upon. We must strengthen the technical communities who maintain foundational software, and strategically support those open source technologies that are aligned with our industrial, regulatory, and societal goals. In the automotive sector, this could mean co-investing in software stacks that power electric vehicles and autonomous driving systems, or in tools that improve functional safety and software lifecycle compliance.

Open source is more than a software model – it is a mode of collaboration that fits Europe's values. But it requires leadership, stewardship, and coordination. Mercedes-Benz is proud to support efforts to build a more sustainable and resilient open source ecosystem. We hope this study inspires others to join the conversation and support this important work.

Magnus Östberg
Chief Software Officer, Mercedes-Benz AG

Markus Rettstatt
Vice President Software Defined Car, Mercedes-Benz Tech Innovation GmbH

Foreword by SAP

The EU Sovereign Tech Fund (EU-STF) initiative from OpenForum Europe (OFE) represents a pivotal step toward ensuring the sustainability, security, and resilience of open source software (OSS) – a cornerstone of Europe's digital infrastructure and a catalyst for innovation. A robust, EU-wide fund, backed by the public sector, is essential to support the maintenance of open source projects and to prioritize those in the public interest, addressing gaps that the private sector alone might not be able to fill sufficiently.

SAP's commitment to open source is deeply rooted in our history and vision. We actively support our employees in creating both bug fixes and feature contributions to open source projects, fostering a culture of collaboration and innovation. In addition, SAP is establishing its own open source funding mechanism to support smaller third-party projects vital to our stack – particularly those with limited resources and maintainers. As an active participant in EU's IPCEI-CIS initiative we contribute to developing open, interoperable, and cloud infrastructure for use in Sovereign Services through the Apeiro Reference Architecture project. Based on this initiative, SAP showed leadership in co-founding the NeoNephos Foundation, which reflects our commitment to fostering open cloud ecosystems that prioritise security, scalability, and digital sovereignty. In addition, we financially support and collaborate with numerous open source foundations, reinforcing transparent governance and ecosystem trust.

These private-sector initiatives – grounded in innovation and driven by expertise – complement what public funding can uniquely provide: structured, large-scale, and strategic support for priorities across the entire ecosystem. In contrast to the private sector, which may focus on proprietary interests or neglect less visible maintenance efforts, a publicly funded initiative can provide consistent support for projects that serve the public interest, such as those addressing cybersecurity risks. By introducing government-backed funding via the EU-STF initiative, Europe can elevate open source to a truly resilient, sovereign digital infrastructure. This synergy assures long-term security, enhances freedom of choice, and empowers both public services and European businesses. Germany's Sovereign Tech Fund/ Agency might serve as template for the EU-STF. Launched in 2022, it follows similar goals and has already invested over €23.5 million into more than 60 open source projects.

This study, conducted with Fraunhofer ISI and the European University Institute, provides a roadmap for the EU-STF, ensuring it secures the digital infrastructure that underpins our shared prosperity. We look forward to collaborating with policymakers, industry partners, and the open source community to bring this vision to life.

Peter Giese

Director of SAP Open Source Program Officer

Table of Contents

Glossary

AI	Artificial Intelligence
AIA	AI Act
ALT-EDIC	The Alliance for Language Technologies of Good Practices.
BBI JU	Bio-Based Industries JU (Joint Undertaking)
CA JU	Clean Aviation JU (Joint Undertaking)
CBE	Circular Bio-based JU
CEF	Connecting Europe Facility
CINEA	European Climate, Infrastructure and Environment Executive Agency
CLARIN-ERIC	Common Language Resources and Technology Infrastructure ERIC (European Research Infrastructure Consortium)
CRA	EU Cyber Resilience Act
CSA	EU Cyber Security Act
CSC-EDIC	Digital Commons EDIC and a Cybersecurity Skills Coalition EDIC
CSIRT	Computer Security Incident Response Team
DARPA	Defense Advanced Research Projects Agency
DCD	Digital Content Directive
DEFIS	Defence Industry and Space
DESI	Digital Economy and Society Index
DG	Directorate-General
DG-CNECT	European Commission Directorate-General for Communications Networks, Content and Technology
DG-COMP	European Commission Directorate-General for Competition
DG-DIGIT	European Commission Directorate-General for Digital Services
DG-GROW	European Commission Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
DG-DIGIT	Directorate-General for Digital Services
DG-RTD	Directorate-General for Research and Innovation
DG-SANTE	Directorate-General for Health and Food Safety
DIGITAL	Digital Europe Programme
DMA	Digital Markets Act
DSA	Digital Services Act
DSM	Digital Single Market

EBSI	European Blockchain Services Infrastructure
EC	European Commission
EC-OSPO	European Commission Open Source Programme Office
ECCC	European Cybersecurity Competence Centre and Network
ECSEL	Electronics Components and Systems for European Leadership
EDCTP	European & Developing Countries Clinical Trials Partnership
EDIC	European Digital Infrastructure Consortium
EDIEA	European Digital Infrastructure Executive Agency
EEA	European Economic Area
EIC	European Innovation Council
EISMEA	European Innovation Council and SMEs Executive Agency
ENISA	The European Union Agency for Cybersecurity
EU	European Union
EU-FOSSA	EU Free and Open Source Software Auditing
EU-FOSSA-2	EU Free and Open Source Software Auditing 2
EU-STF	EU Soverign Tech Fund
EUI	European University Institute
EUOPEUM-EDIC	European Blockchain Partnership and European Blockchain Service Infrastructure EDIC (European Digital Infrastructure Consortium)
EUVDB	EU Vulnerability Database
FSTP	Financial Support to Third Parties
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GNOME	GNU Network Object Model Environment
GPAI	General Purpose AI
HaDEA	Health and Digital Executive Agency
IPCEI(s)	Important Project(s) of Common European Interest
IPCEI-ME/CT	IPCEI on Microelectronics and Communication Technologies
ISI	Institut für System
IT	Information Technology

JEDI	Joint European Disruptive Initiative
JEF-IPCEI	Joint European Forum for IPCEI
JU(s)	Joint Undertaking(s)
LDT CitiVERSE EDIC	Networked Local Digital Twins towards the CitiVERSE EDIC (European Digital Infrastructure Consortium)
LUMI	Large Unified Modern Infrastructure
MCP(s)	Multi-Country Project(s)
MFF	Multiannual Financial Framework
MIIT	Chinese Ministry of Industry and Information Technology
NGI	Next Generation Internet
NIS2	Network and Information Systems Directive 2
ODBTs	Open Digital Base Technologies
OFE	OpenForum Europe
OIS	Open Internet Stack
OSH	Open Source Hardware
OSPO	Open Source Programme Office
OSS	Open Source Software
PLD	Product Liability Directive
SESAR JU	Single European Sky ATM Research (SESAR) Joint Undertaking)
SME(s)	Small and Medium Enterprise(s)
SNS JU	European Smart Networks and Services JU (Joint Undertaking)
SP	IEEE Symposium on Security and Privacy
SPRIND	Federal Agency for Disruptive Innovation
SRIA	Strategic Research and Innovation Agenda
STF	Sovereign Tech Fund
TEN-T	European Transport Network
TFEU	Treaty on the Functioning of the European Union
TSMC	Taiwan Semiconductor Manufacturing Company
US	United States
VAT	Value-Added Tax

Executive Summary

This feasibility study reveals deep pockets of political will and momentum for the establishment of an EU Sovereign Tech Fund (EU-STF).

Chronic under-investment in open source technologies creates systemic risks – exposing Europe to (amongst other things) cybersecurity threats, supply chain vulnerabilities, and strategic dependencies on non-European technology providers. In order to maintain, secure, and improve existing open source technologies to meet the EU's public and industrial goals, it requires policymakers to understand the logics underpinning failures in investing in the maintenance of open source technologies as open digital infrastructure, in order to prioritise the use of public policy towards the unlocking of financial and non-financial resources that support the open source ecosystem.

The EU-STF is envisioned as a scaled-up, pan-European, and mission-driven initiative with a proposed budget of at least EUR €350 million over seven years to invest in maintenance, security, and improvement of key open source components, as well as help identify and map dependencies and invest in ecosystem strengthening activities. It is vital that the EU-STF embodies some key principles (many of which have made the German successful): pooled financing, low bureaucracy, political independence, flexible funding, community focus, strategic alignment, and transparency.

To this end, it has been determined that two active budgetary scenarios are worth considering for the EU-STF: (1) a standalone and centralised fund (e.g. a new funding body created by legislation and set aside via the MFF negotiations), and (2) a hybrid/shared management structure (such as leveraging established EU institutional frameworks like the EDIC that allow for pooled contributions of Member States alongside EU funding, and even industry co-financing). These options are not necessarily mutually exclusive either. No single approach offers the most viable path and each has its own advantages as well as trade-offs.

On the one hand, the hybrid/shared management structure models offer distinct advantages in flexibility and preservation of the character of the German STF, and would not require legislation or a legislative amendment (as compared to a standalone and centralised fund). On the other hand, the standalone and centralised fund offers distinct advantages in terms of unlocking a significant volume of capital, improving public recognition of the challenge, and prominently showcasing the mission-driven nature of the EU-STF.

To implement the vision for an EU-STF, we issue a call-to-action to the EU and its Member States to act with urgency in considering these two budgetary scenarios and the related recommendations, recognising that fragmented, uncoordinated, or siloed efforts will not be sufficient to unlock funding for open digital infrastructure which addresses Europe's digital challenges. We call for their contribution to this important and timely fund, which would be complemented with additional external sources of funding including from the private sector rather than place the budgetary onus exclusively on the EU. That diversification of funding furthers sustainability and buy-in from relevant stakeholders to overcome these systemic challenges.

I. Introduction: The 21st Century Digital Infrastructure Responsibilities of Governments

The digital transformation of modern society has reshaped the responsibilities of governments. What is considered infrastructure – roads, bridges, power grids, etc – now needs to include software systems that underpin public services, economic activity, and democratic institutions.

At the heart of this digital infrastructure, there are foundational software components deeply embedded across digital systems – from communications and healthcare to mobility, finance, and energy. These systems are frequently built on open source software (OSS), software components with source code that anyone can inspect, use, modify, and enhance.[1] Because of these attributes, it is taken for granted, despite it being foundational for all modern software development. As a result, the maintenance of these components remains largely under-resourced, often run by technical communities on a volunteer basis, as passion projects, or on top of their day jobs.

OSS components are proven foundational for the digital infrastructure we all rely on. But their deep and foundational contributions to the digital infrastructure we all rely on have not been accompanied by an equal focus on sustaining and investing in them. In many cases, critical OSS is developed and maintained with limited or no financial support, despite being foundational and taken for granted at the heart of national and European digital strategies.

The value society derives from OSS is immense and the scale of funding – from both the public sector and industry – has not grown commensurate with its impact. What we see in this dilemma is a fundamental mismatch between the societal value in relying on OSS as digital infrastructure and the level of investment it receives. Public-led funding of OSS offers a different source of funding which is not mutually exclusive with private funding. The logics underpinning private investment in OSS have broadly worked in sustaining the open source ecosystem, but have failed to create pathways for sustaining projects with major systemic impacts, creating risks to the infrastructure that depends on them.

Our proposal is to build an EU Sovereign Tech Fund (EU-STF),[2] an institution contributing to this responsibility and which shows that the European Union (EU) is willing to base its digital sovereignty, cybersecurity/cyber resilience, and competitiveness on sustainable and secure open source technologies. The EU-STF would not just offer public funding for open source, but lead different actors – including Member States and industry – in diversifying funding and investment into the open source ecosystem. Such an effort is needed not only for the sake of broader ecosystem health, but to safeguard against episodic security incidents and the negative externalities of under-investing in routine maintenance of key libraries, packages, and applications –

which all European digital infrastructure depends on.

As the culmination of an in-depth study, this report offers a detailed assessment of its economic, legal, and political feasibility of the EUJ-STF. It makes a high-level case for the EU-STF (Section II), explains in detail a political and economic rationale for greater investment in open source technologies (Section III), explores some design considerations for the EU-STF (Section IV), provides an overview of its legal feasibility (Section V), and summarises some recommendations for how to make it happen politically (Section VI). As we will show, the EU-STF offers a vehicle, fit for the realities of the 21st century, to align Europe's digital policy ambitions with sustained investment in open source technologies.

II. Proposal: The Establishment of an EU Sovereign Tech Fund

This section overviews the high-level case and proposal for an EU-STF. To start, we survey how critical open source technology is maintained today (Section 2.1), the problem of persuasion at heart of the open source maintenance crisis (Section 2.2), and the history of the German STF (Section 2.3), before making a case for the unique and distinguishing features of an EU-STF (Section 2.4) and summarising the methodology for this feasibility study (Section 2.5).

2.1. Context: How our Critical Open Source Software is Maintained Today

Software is a set of instructions that tells a computer what to do. These instructions are written in programming languages and are often bundled into libraries, packages, or applications so developers do not have to rebuild the same functionality over and over. Virtually all modern software – whether powering websites, smartphones, cloud platforms, or critical public infrastructure – relies on OSS or OSS components somewhere in its stack. Since OSS components and the libraries, packages, and applications that are built on them are freely available, collaboratively developed, and legally reusable, they are the invisible backbone of nearly all digital innovation.

The scale of the need to maintain, secure, and support such technologies is immense. More than 70% of modern software depends on OSS and OSS components.[3] The security and sustainability of society's open source dependencies is no longer just a technical issue – it has become a matter of acute public interest, with strategic and geopolitical dimensions. This is because the layered structure of software creates a 'dependency tree', with each layer of software depending on many others to function correctly. A single application might rely on hundreds – or even thousands – of open source components, libraries, packages, or applications, all of which are maintained by communities distributed around the globe.

When foundational open source components are outdated, insecure, or abandoned, they can compromise the stability of entire systems that depend on them. This can happen for many reasons, including a lack of time, a decline in interest, or even burnout of contributors. Digital systems must be constantly updated for security, compatibility, and performance. Software does not just exist – it has to be actively maintained.[4] However, the maintenance burden often falls to ad-hoc support from companies, the committed efforts of passionate volunteers, or the dogged efforts of a handful of open source foundations[5]

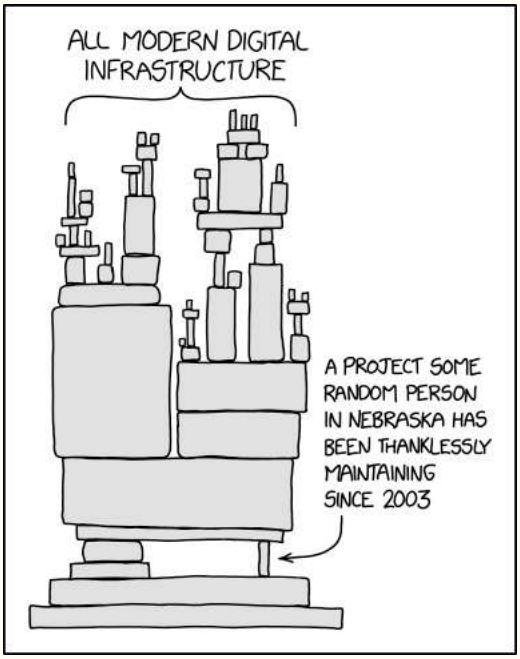

Figure 1. This classic XKCD comic highlights the common dynamics of society's collective reliance on the work of open source maintainers. (Source: CC-BY-NC 2.5 XKCD)[6]

These dynamics create a structural imbalance where the benefits of open source are widely distributed, but the burden of upkeep falls on just a few individuals, communities, and organisations. While many projects make this work, not all do. Investing in open source maintainers is thus not only a question of digital resilience but of long-term public interest. It is imperative that we act on the need to proactively maintain and secure these open source technologies and create a more diverse pool of funding which supports their sustainability.

2.2. Challenge: The Problem of Persuasion at the Heart of the Open Source Software Maintenance Crisis

Convincing policymakers (and industry) to invest in the sustainability, maintenance, and security, and support of open source technologies is a problem of persuasion. Efficient and innovative open source collaboration and development activities have been happening for decades; they just need to be supported and invested at greater scale. While this challenge is not new for the open source community, it remains something that society at large – including key decision-makers – find difficult to grasp.

Nadia Eghbal's seminal 'Roads and Bridges' report first outlined the key aspects of this challenge.[7] It described OSS projects as a form of digital infrastructure[8] that should be treated as a public good, not a free resource. Despite this understanding being widely accepted, OSS is plagued by a complicated tragedy of the commons, leading it to be undervalued and under-invested. This complacency with the status quo is a political challenge, and the failure to address it has been a matter of public policy, not a fault of the open source ecosystem.

It is not specific to Europe either. With few exceptions, open source technology suffers from a visibility problem: it works so well, so seamlessly, that its fragility remains hidden until something breaks, particularly in the eyes of governments. Because it is freely available and developed outside traditional market structures, many public and private actors mistakenly assume 'someone else' is taking care of it.

The last years of digital history have made it clear that it's time for that to change. We must develop a more persuasive case for funding open source maintainers to keep doing the work they are already doing; not as an act of charity or tech philanthropy, but as a pragmatic and cost-effective investment in the infrastructure we all depend on. This is a public interest and solvable challenge, if only governments and industry can be convinced that supporting maintainers is a way to prevent future crises, not merely respond to them.

Europe is well-positioned to rise to this challenge. In Europe, a long history with integrating open source into public administration and leveraging open standards has increased awareness of open source compared to other regions of the world. Tthe importance of OSS in the public sector in Europe is widely acknowledged in ministerial declarations[9] and by the European Commission (EC) through its establishment of an open source programme office (OSPO).[10]

In this sense, Europeans seem to be broadly persuadable on this issue. It might just be a matter of coming together around a new vision for open source investment. This should start by using the right metaphors and tools for comparison. A helpful metaphor is that of open source technology as open digital infrastructure, building on the line of thinking put forth by Nadia Eghbal. Policymakers must ground their understanding of open digital infrastructure in real-world precedents for physical infrastructure – which many have an easier time grasping due to their more visible and non-technical nature.

No analogy from the physical world is perfect, but parallels can be drawn between open source technologies in society and other aspects of societal infrastructure. These include:[11]

- **Water Management:** OSS and OSS components are vital to digital ecosystems, much like water to physical ones. The immense variety of interlinking use cases from a common resource highlights the importance of maintaining ecosystem health.

- **Capital Markets:** Both capital markets and OSS create systemic risk through leverage and dependency. They serve as enabling inputs for essentially all areas of social and economic activity, underscoring the need for transparency and targeted support.

- **Roads and Bridges:** Like critical transportation infrastructure, OSS and OSS components require maintenance that correlates with its criticality and usage. Investment by a few benefits many, and maintenance is crucial to prevent catastrophic failures.

Unlike open digital infrastructure, physical infrastructures receive substantial attention and funding from policymakers in Europe. In these examples, that is true through initiatives like the EU Water and Waste Framework Directives,[14] the European Securities and Markets Authority,[15] and the Connecting Europe Facility (CEF) and Cohesion Fund.[16] So, where is the structured public funding for the open source ecosystem?

System	Estimated Annual Budget (€)
Air Quality (AQI + CAMS + JRC)	EUR €160–220 million
Water Quality Calibration	EUR €65–130 million
Aviation Safety (EASA + Eurocontrol)	EUR €50–80 million (EASA); EUR €500 million+(Eurocontrol)

Instrument	Estimated Annual Budget (€)
EASA[12]	2024: EUR €243 million (EUR €45 million EU subsidy, rest: revenues)
Eurocontrol[13]	2023: cost base: EUR €511 million, budget: EUR €180 million, result - EUR €86 million

Figure 2. Budget estimates for physical infrastructure. (Source: Authored; Sourced from instrument websites)

2.3. Paying Maintainers to Do Their Work: Context on the German Sovereign Tech Fund/Agency and Its Model

The German Sovereign Tech Fund (STF) launched in October 2022. Its goal is to provide structured funding for the open source ecosystem and invest in this open digital infrastructure. The fund's launch of the fund was two years in the making and followed an approval of initial funding by the German Bundestag in May of that year.[17] The fund addresses the long-standing challenge of under-investment in open source technology, although specifically without bias towards end-user applications and services and with a focus on foundational digital technologies that enable the creation of software.

The German STF pivoted away from end-user applications and services, which receive much more support and attention – and instead specifically invested in Open Digital Base Technologies (ODBTs).[18] These ODBTs are foundational digital technologies underneath applications and services which enable the creation and execution of software on operating and networked communications systems. Recognising that not all open source technologies but specifically ODBTs form the backbone of modern digital infrastructure, the STF provides dedicated, strategic funding for projects underpinning Germany's and Europe's digital sovereignty. This is an alternative focus to the private, volunteer, and market-driven sustainability efforts that normally guide much open source funding. It is also a focus which has been central to the procurement logic of the German STF, which procures maintainers directly to do essential maintenance and development work on their projects.

Because of an innovative setup and mandate, the German STF is now a critical catalyst and emblem of innovation in the open source funding landscape. It regularly highlights the need for sustained, long-term investment in ODBTs as open digital infrastructure, as well as innovates in its focus on public funding of ODBTs. Through direct financial support to maintainers, the German STF has empowered a wide range of open source projects critical to the digital economy. These are projects which might otherwise struggle to secure adequate funding through commercial channels alone. By focusing on sustainability and projects of strategic importance, the German STF ensures that key open source components remain actively maintained and resilient against emerging threats, complementing private-led and market-driven sustainability models.

The STF's investments in open digital infrastructure support the security, stability, and reusability of many ODBTs, bolstering the open source ecosystem in Germany and beyond. A key feature of the STF's approach has been its emphasis on community-driven development and governance. Rather than dictating project direction from the top down, the STF works in partnership with maintainers and developers to identify the most pressing needs and opportunities for intervention. This approach respects the decentralised nature of the open source ecosystem while providing institutional support and financial resources that many projects lack. It also means that the STF plays a key role in ecosystem strengthening and awareness raising in the open source community.

Recognising the scale and importance of its mission, the STF was given a permanent home at the newly established Sovereign Tech Agency, itself a permanent institution tasked with stewarding these investments over the long-term. The transition to an agency structure reflects the growing recognition that digital sovereignty and security are strategic imperatives requiring sustained, coordinated action at the (supra-)national level, with inputs from the global open source ecosystem. The Sovereign Tech Agency's expanded mandate includes not only direct funding of open source projects but also fostering greater collaboration between government, industry, and the open source community.

2.4. From a German to an EU Sovereign Tech Fund

The work of the German STF and its evolution into the Sovereign Tech Agency provide a valuable blueprint for such a fund being set up EU-wide. The success of the German STF – demonstrable, but also limited by its funding – underscores the need for an EU-STF, which can increase the scale and mandate of these investments while extending the benefits. Such a fund would invite greater contributions from other public sector actors, industrial players, and small and medium enterprises (SMEs). Scaling up the funding and mandate will ensure even more than before that the entire continent can share in the security, innovation, and resilience that robust open source ecosystems enable.

We propose that the establishment of the EU-STF should be modelled closely on the German STF – with only small differences in terms of points of emphasis and strategic positioning – and that is should support key European digital policy ambitions like digital sovereignty, cybersecurity/cyber resilience, and competitiveness. Investment in open digital infrastructure supports sovereignty not by enabling digital sovereignty itself, e.g. separating supply chains and dependencies through this investment, but by supporting the foundational aspects of sovereignty: security, innovation, autonomy, resilience, competitiveness. This argument is distinct and related, but complementary, to the many calls for digital sovereignty argued by groups like the EuroStack initiative.19 (A more detailed argument for

this will be advanced in Section 3.1 and 3.2.)

In advancing these political goals, we make the case that investing in open digital infrastructure through an EU-STF will be structurally transformative and mission-driven. Rooted in salient aspects of the EU's 'digital political economy', it will transform how digital technology is invested in, have a very high return on investment, and embrace a mission-driven orientation for addressing European challenges. A strategic investment in scaling up the German model will support European digital infrastructure but also the entire global open source ecosystem (A more detailed argument for this will be advanced in Section 3.3 and 3.4.).

Such an effort must preserve the core features of the German STF while embracing distinguishing aspects of its EU-wide scale. It should have a proposed budget of at least EUR €350 million (contributed by the EC) to invest in maintenance, security, and improvement of key open source components, as well as identify/map dependencies and invest in ecosystem strengthening activities. Based on the findings of the interviews for this study, it should also enable: pooled financing, low administrative burden, political independence, flexible funding, community focus, strategic alignment with policy objectives, and transparency.20 (A more detailed argument for this will be advanced in Section IV.)

To arrive at an assessment of the feasibility of an EU-STF (see Sections V and VI), the study employed a mixed-methods approach to assess the opportunity and feasibility of establishing an EU-STF, e.g. a EU-wide funding instrument modeled after the German STF. The methodology provided robust, evidence-based and politically viable recommendations within EU institutional frameworks suitable for integration into the EU's next Multiannual Financial Framework (MFF) package negotiations, which begin in July 2025 and will determine the seven years of funding from the EU budget in the period 2028-2034.

2.5. A Brief Note on the Methodology for this Study

The study employed a non-linear integrative mixed methods research approach. This approach is based on a teamwork development process21 where responsibilities for particular aspects of the feasibility were assessed. A team from Fraunhofer ISI22 considered the economic feasibility of the fund, a team from the European University Institute23 (EUI) considered the legal feasibility of the fund, and a team from OpenForum Europe24 (OFE) considered the political feasibility of the fund. OFE led the writing and synthesis of these insights to final publication.

The methodology was structured around two parallel research phases, which were integrated at the end. The first phase consisted of a landscape assessment examining the current state of OSS sustainability and security challenges across Europe with a series of interviews. The second phase focused on economic analysis and implementation feasibility, evaluating several distinct institutional scenarios.

For the first phase, data collection centered on semi-structured interviews with 26 stakeholders across 23 interviews. These interviews represented a diverse range of stakeholder groups, including EU institutions, EU industry, Member State cybersecurity agencies, cybersecurity and digital policy experts/ researchers, funders, and technical communities. Two collaborative workshops supplemented the interview process.

For the second phase, the analysis combined qualitative and quantitative economic assessment with institutional analysis and qualitative analysis of stakeholder interviews gathered as part of the parallel research phase. Economic evaluation created a detailed political and economic argument for the fund, rooted in literature and European experiences, as well as estimated funding needs by extrapolating from German STF experience to EU-wide scale. Legal feasibility analysed various categories of institutional setups, examined treaty bases for different institutional arrangements, and assessed coordination requirements with existing EU programmes and bodies.

The study faces several limitations which should be noted in consideration of its generalisability. These primarily centred on constrained data availability on EU-wide OSS dependencies, limited quantitative modeling time due to data availability issues,25 MFF deadline requirements,26 and evolving political dynamics affecting stakeholder positions. Ethical considerations ensured stakeholder confidentiality with findings reported in aggregate form, without pseudonymised or anonymised attribution.

III. Political and Economic Rationale for a European Sovereign Tech Fund

This section makes a detailed and evidence-based political and economic argument for the EU-STF. It uses the lens of 'digital political economy' to consider how the EU-STF ought to be situated in the current digital policy landscape in Europe (in Section 3.1), before then making a case for mission-driven investment (in Section 3.2). While not exhaustive, it asserts that the positioning of the EU-STF is vital for advancing key digital policy objectives, in support of much broader European goals around competition and simplification of investment.

3.1. The EU's 'digital political economy': Digital sovereignty, cyber resilience, competitiveness

In recent years, EU digital policy has been dominated by an intense wave of legislative activity and enforcement efforts.[27] These have most notably included the landmark Digital Services Act (DSA) and Digital Markets Act (DMA) enacted in mid-2022,[28] alongside the implementation of the General Data Protection Regulation (GDPR), which has tried (to mixed results)[29] to address data protection abuses and the concentration of power in digital markets.[30] In recent months, however, digital policymaking in Brussels has consolidated around a few key themes following the election of the new EC: digital sovereignty, cybersecurity/cyber resilience, and competitiveness. Understanding these themes lays the foundation for understanding the potential scope and impact of an EU-STF in the current political climate.

3.1.1. Digital sovereignty

Digital sovereignty has many definitions, but at its core, it is about ensuring that information technology users – from individuals to industry to governments – can switch away from dominant vendors and have credible alternatives to turn to. While recent regulatory efforts like the DMA and the Data Act have addressed the ability to exit, attention is now shifting toward how policy can help build the alternatives worth switching to. Instead, it might be worth thinking about how to maintain the alternatives that already exist, much of which is available as OSS. Digital sovereignty should not mean technological isolation, and investing in open source is one of the few ways to ensure sovereignty does not come at the cost of agility, innovation, or relevance.

There are two key reasons why funding open source technologies is connected to the conversation on digital sovereignty. First, they allow governments to be autonomous, e.g. have the freedom to choose more open alternatives which enable interoperability, competition, and collaboration without lock-in. Second, the EU must strengthen its capacity to manage and maintain the software infrastructure it increasingly relies on, in turn allowing it to become more resilient. Both are urgent policy imperatives, and targeted support for open through an EU-STF addresses them by reinforcing Europe's ability to shape, govern, and sustain its digital capabilities.

As of early 2025, many topics related to digital policy seem to flow from digital sovereignty, with broad support across many EU political institutions.[31] This was not a given as of early 2024. Since then, the movement towards rhetoric around ideas like 'digital independence'[32] has consolidated following the upheaval and uncertainty kicked off by the new Donald Trump administration in the United States (US). Yet this is not always accompanied by the inflammatory rhetoric some might imagine. As recently as June 2025, Henna Virkkunen – the new Executive Vice President for Tech Sovereignty, Security and Democracy – has positioned Europe's path towards digital sovereignty as the embodiment of calm and reason.[33]

In the race for the advancement and deployment of new digital technologies and AI, Europe still lags behind its biggest competitors, primarily the US and China (IMD, 2024). While some Member States are slowly increasing their digital competitiveness[34] and individual European companies are globally successful,[35] Europe remains largely dependent on non-European suppliers of digital services, platforms, and the underlying supply chains for its digital economy.[36] With the Digital Decade programme[37] the EU has set ambitious targets to reduce this dependency by 2030 and strengthen European digital competitiveness and resilience. Together with other regulative acts like the AI Act (AIA),[38] the European Chips Act,[39] and the DMA,[40] and flanked by investment and funding programmes such as the Digital Europe Programme (DIGITAL)[41] or Horizon Europe,[42] this signals the urgency which the EU (as well as its Member States) see in closing the capability gap towards international competition for the digital economy.

These lofty ambitions towards digital sovereignty manifest in pan-European projects and new proposed legislation as well. Projects like Gaia-X[43] and the EU Digital Identity Wallet44 are built upon and rely heavily on trusted OSS components with the goal of helping Europe become independent in critical functionalities. New legislation, like the EU Cloud and AI Development Act,45 embodies a critical step in Europe's pursuit of digital sovereignty by establishing governance frameworks and technical standards for cloud and artificial intelligence (AI) services that align with European values and interests. European leaders, including French President Emmanuel Macron[46] and recent German Chancellor Olaf Scholz, have repeatedly emphasised the need to reduce over-dependency on a small number of digital infrastructure providers, many of whom operate in highly concentrated global markets.[47]

These commitments are made clear through the recent initiatives of Member States. These include, for example, France's advocacy and investment in Digital Commons[48] and Germany's commitment to the STF and its own Center for Digital Sovereignty (ZenDiS).[49] More recently, Denmark's Ministry for Digital Affairs has begun replacing Microsoft Office with the open source LibreOffice, part of a broader push toward digital sovereignty that includes evaluating Linux alternatives and reducing dependence on US-based tech providers.[50] Such initiatives underline how these types of ambitions can be operationalised as part of the day-to-day work of digital governance and public administration.

Despite these successes, the long-term impacts of specific technology decisions and how they are procured remains uncertains. In fact, as Europe accelerates its digital sovereignty agenda, there is a risk that the urgency to build European alternatives could repeat the mistakes of the past. In the rush to replace lock-in, the EU may fall into a new form of dependency – this time on European vendors that, while domestic, are closed-source, commercially siloed, and structurally unprepared to compete globally.

Rather than competing on the terms set by incumbents, Europe should build on these precedents and embrace open source and open standards as the foundation for rebuilding digital autonomy and resilience. As opposed to a simple 'Buy European' approach, investing in open digital infrastructure would reduce barriers to entry, increase interoperability, and foster collaboration across borders. Such investments are not just a tool of governance or ideology, but a pragmatic strategy for enabling autonomy and resilience, as well as regaining technological leverage in a world where the dominant platforms were not made in Europe.

By leveraging OSS for digital sovereignty, the EU will help avoid the costliest forms of vendor lock-in, strengthening its autonomy and resilience and creating a foundation for longer-term impact. OSS allows multiple providers to compete based on the same core code, thus facilitating autonomy and resilience (more on these concepts in Section 3.1.2). This approach helps Europe reduce technology and supplier dependencies while developing internal capabilities to set standards, support its digital transformation, and uphold European values.[51] In practice, investing 'upstream' in OSS – whether through capacity building, public-sector open source offices, or targeted funding – delivers powerful 'downstream' effects: robust, sovereign, and more open digital infrastructure that the EU can govern, secure, and evolve on its own terms.

3.1.2. Cybersecurity/cyber resilience

Cybersecurity and digital sovereignty are deeply intertwined, often through the use of the term 'cyber resilience'. EU policy has evolved significantly with the Network and Information Systems Directive 2 (NIS2 Directive, or NIS2),[52] the EU Cybersecurity Act (CSA),[53] and particularly the newly adopted Cyber Resilience Act (CRA) – which imposes stricter security obligations on manufacturers and retailers of products with digital elements.

Many OSS projects are currently unable to meet these new standards – though it is important to note that not all OSS projects would be required to do so. The CRA provides a general exemption for OSS developed for non-commercial purposes, and introduces a 'light-touch and tailor-made' regime for OSS stewards; these are defined as legal entities which support development but not deployment of OSS for commercial use.[54] The primary obligations fall on manufacturers or other entities deploying OSS commercially. Nevertheless, for those that do face the obligations of meeting new standards under the CRA, a 2024 survey of open source maintainers – half of whom are based in Europe – found that 60% of maintainers are unpaid, and most are the sole maintainers of their projects.[55] While securing software upstream through targeted investment would reduce risk across the ecosystem, it would not exempt downstream SMEs from their obligations under the CRA or other legislation, and maintainers themselves are (in most cases) not considered manufacturers under the regulation's definition.

These structural challenges demonstrate the criticality of investing in open source communities as a vital strategic objective essential for fulfilling and enabling compliance with the legislation. Experts on cybersecurity around the world are alarmed by the European dependency in the global software stack and the resulting potential for threats to the software supply chains through dependencies. Tthis dependency through software supply chains has been named as the number one cybersecurity threat by the European Union Agency for Cybersecurity (ENISA) in their foresight reports.56 The fact that there is a dependency on foreign software and digital service components potentially allows non-European

actors to control their usage and application, with potentially detrimental effects to users and companies, as well as the EU and its Member States.

One of the most critical aspects of these dependencies is less obvious at first glance. Publicly available open source programmes and libraries of code are regularly used and reused as building blocks of many different applications.[57] These OSS libraries are of central importance to the digital economy, with a demand side value of up to USD $8.8 trillion and delivering major cost savings for commercial operators compared to independent development.[58]

While OSS and open source libraries are regularly scanned for vulnerabilities, they are still a major security risk once integrated in interdependent software interfaces.[59] Left unattended, this enables certain actors to compromise the supply chain by inserting backdoors and malign code to create political, financial, and intelligence threats.[60] One example of the potential danger caused by such backdoors is the partially successful manipulation of the XZ Utils software[61] – a data compression algorithm used mainly by Unix[62]-based systems – which if not discovered early, would have compromised computers and servers globally.[63]

Attacks on the open source supply chain are a major threat to the digital security of Europe. This threat is further multiplied by the relative ease with which the open source supply chain can be manipulated by malignant actors by a mix of social engineering and targeted downstream insertion in interdependent software packages used as building blocks for many higher-level applications.[64] [65] Two examples of this are 'Zero Day vulnerabilities'[66] – which are often the result of systemic under=investment in maintenance and lack of dedicated security review, resulting in ease of malicious targeting – and the deliberate insertion of malicious backdoors,[67] which typically involve targeted attacks exploiting the trust-based nature of open source contribution.

Improved ways to enhance the security and resilience of software supply chains are needed. Commercial actors as well as individual programmers have significant interest in contributing and using OSS.[68] Free-riding possibilities – or the simple lack of a business interest in specific areas of software development and sustainable long-term support of OSS projects – are leading to insufficient commercial incentives to contribute especially to the maintenance and security review necessary to establish increased cybersecurity in OSS.[69] [70] [71]

A further wrinkle comes from the impact of pending cybersecurity legislation on open source innovation and developer engagement. For example, the CRA's strict security expectations highlight a larger systemic challenge: open source maintainers are shouldering an ever-growing security and maintenance burden without corresponding financial or institutional support.[72] That investment is necessary to increase the possibility for smooth implementation of the legislation, which was softened to better accommodate (albeit imperfectly) the needs of the open source ecosystem. With targeted investment and support, the EU-STF can help facilitate stronger, more secure and resilient software supply chains by easing the burden of compliance for critical projects, in keeping with the spirit and objectives of the CRA.

Policymakers therefore face a strategic imperative: to complement regulatory measures like the CRA with concrete investments in capacity building, funding mechanisms, and collaborative security initiatives. This must not only empower open source communities around the edges, but maintain, secure, and improve the open source fundamentals, with improved cybersecurity and cyber resilience naturally following. The EU-STF should also support CRA compliance by channelling targeted investments into open source maintenance and security auditing upstream, thus maximising return on investment by decreasing the compliance burden of all downstream users of those dependencies.

3.1.3 Competitiveness

OSS as a driver of competitiveness is not a new paradigm globally, or a paradigm specific to Europe. Many countries have doubled down on open source technologies as part of their economic and digital strategies.[73] Reflecting a growing awareness and interest amongst governments in open source technologies as open digital infrastructure that can further one's digital interoperability, autonomy and innovation, many countries are adopting policies that support and/or promote investment in OSS. (China[74] and South Korea[75] are examples of countries that have recently adopted policies and invested in OSS.)[76]

In Europe, open source technologies are not just a technological asset but an essential pillar of the continent's economy, including its innovation and competitiveness. Harvard Business School research concludes that without OSS and its supporting developer networks, companies would need to spend 3.5 times more on software development, amounting to an estimated USD $8.8 trillion globally.[77] Based on what we know of the value and reach of OSS in Europe (more on this below) the potential societal and economic impacts of vulnerabilities in OSS and OSS components are huge. Furthermore, the benefits of increased trust in OSS – from both European industry and its SMEs – would likely have a demonstrable effect in supporting its business and innovation ecosystem, bolstering (digital) competitiveness.[78]

For strategic European industries such as automotive and telecoms, OSS is not merely a cost-saving tool but a foundation for collaborative innovation and long-term digital competitiveness. The automotive sector has recently underscored this strategic importance through a Memorandum of Understanding signed by major manufacturers and suppliers to jointly develop and maintain OSS for car systems, recognising that shared development of core software components accelerates innovation while reducing duplication of effort.[79] Strengthening OSS maintenance and security in these critical ecosystems would therefore have an outsized positive impact, not just by safeguarding supply chains but by reinforcing Europe's competitive edge in sectors where it is already a global leader.

OSS is not only essential to the resiliency and security of software supply chains, but offers significant efficiency gains for the commercial sector and the whole economy.[80] [81] A 2021 EC study further validates this perspective, showing that investing in OSS sustains not only digital innovation but economic growth. Companies within the EU invested approximately EUR €1 billion in OSS in 2018, resulting in an economic impact estimated between EUR €65 and EUR €95 billion.[82] This reflects a hard-to-beat cost-benefit ratio, indicating that open source technologies are not only technological assets but a significant economic driver across Europe.

Additionally, a European focus on guiding the development and establishing the sustainability of

open digital infrastructure also holds the potential for enabling the EU to forge its own path in digital transformation. As the developments of the recent years have shown, the normative understanding of how digitalisation should and will be shaping society and economy differ significantly between different global actors. While the US follows a market-driven approach towards digitalisation which is characterised by minimal government involvement and strong competitive elements on the global stage, China – at the other end of the spectrum – seeks to guide the process top-down in a state-led approach, with a strong focus on digital sovereignty, (interpreted to mean 'control' or even autarchy). The EU, meanwhile, follows a rights-driven regulatory model, with the influential global ramifications of their regulatory regimes often referred to (both positively and negatively) as the 'Brussels effect';[83] such terms reflect its market power and voluntary adoption of standards by business as well as civil society.[85] [86]

The argument for OSS as a competitiveness driver is consistent with recent policy pushes for competitiveness within the EU. The Draghi report on EU competitiveness underscores that Europe's long-term prosperity hinges on technological independence and unleashing its capacities for innovation.[87] The literature evidences the idea that OSS is critical to Europe's competitiveness ambitions, as it offers an accessible, collaborative foundation that enables both small startups and large firms to build competitive digital products and make their software supply chains more resilient and secure.[88] Moreover, the EC proposed establishing a European Competitiveness Fund as part of its 2028–2034 budget plan, which will channel investments into strategic technologies, innovation, and digital infrastructure, reinforcing support for industrial leadership and technological sovereignty across the European bloc.[89]

While weaker in navigating these disparate approaches of powerful countries in digital governance when compared to the US or China, the EU can use its comparatively smaller resources to be digitally competitive. By combining support for OSS development through an EU-STF with regulations like the DMA, DSA, or the GDPR, the EU has the chance to strengthen the long-term security and sustainability of OSS, aligning with both the interests of the OSS community and EU policymakers.[90] [91] The need for European action in OSS development through an EU-STF is not only about economic gain, but central to promoting the values of openness, innovation, and interoperability at the heart of the EU's digitalisation strategy.

The value-add is not necessarily in leveraging OSS, which governments have been doing for decades, but in investment and support as key to a long-term vision of competitiveness. The EU could channel its collective effort towards this goal of increased competitiveness by reducing its reliance on software solutions, data infrastructure,s and software supply chains hitherto dominated by non-European commercial actors. This would strengthen domestic actors through lowering their dependency on potential competitors, and enhancing Europe's human resources in the digital space.[92] [93] [94] [95]

3.2. The economics of investing in open source technologies

Investing in open source technologies clearly aligns with EU policy priorities, but it is also important to highlight why public funding in particular is important, and how the lack of investment is rooted in classic market and system failures that justify targeted public intervention. Despite their role as non-rival and non-excludable public goods with significant positive externalities, open source technology is uniquely complex in how it is developed, produced, and consumed. Moreover, its 'under-investment'

reflects traditional market and system failures – such as scaling constraints, risk aversion, and the undervaluation of network effects – all of which demand public-led intervention.

We argue that without public-led intervention,the OSS ecosystem will continue to lack the coordinated, mission-driven investments required to sustain, maintain, and secure ODBTs at scale. There are many other projects which do not get the support they deserve, particularly beneath the application and services layers. Moreover, critical gaps remain because companies focus on projects they deem business-critical, leaving foundational libraries that benefit multiple organisations without dedicated support. Public-led funding can demonstrate leadership and make an important contribution to this mission-driven approach (though it is not intended to replace other funding sources.

3.2.1. A dual tragedy of the commons

OSS and open source hardware (OSH) constitute forms of open innovation. They represent the deliberate opening of the innovation process by a firm, individual, or institution to targeted inflows and outflows of knowledge. This facilitates the use of external ideas to accelerate internal innovation while actively sharing or freely licensing internal knowledge.[96] [97] While the motivation for this openness (at least for commercial actors) is often the creation of new market opportunities, it can lead to the creation of a non-rival and non-excludable product – be it in the form of knowledge, code, software or even infrastructures and hardware.

Such technological artefacts therefore constitute public goods and, due to their digital nature, even global public goods with global effects (Kaul, 2016).[98] [99] [100] In the view of some, the very nature of a public good creates a supposed free-rider problem – the idea that if you cannot exclude someone from using something, they will use it without paying. With OSS, this means that contributors and users (or customers) of that software benefit from OSS without contributing back to its development or maintenance, leading to under-funding and potential project abandonment. (It might be argued that the former should be encouraged, while the latter should be discouraged.)[101]

OSS does not reflect the traditional dynamics of public goods. With OSS, Nadia Eghbal argues that it can sometimes operate as excludable, non-rivalrous 'club goods' in their output, e.g. the code can be made excludable by technical, economic, or platform barriers besides OSS licensing, but typically are not. On the other hand, OSS can also act as a form of commons by sometimes operating as rivalrous, non-excludable 'common pool resources' in their production process, e.g. maintainer attention which is rivalrous and creates sustainability challenges that traditional open innovation frameworks may not fully capture – especially as societal dependency on a given piece of software and, by extension, its maintainer increases. [102]

As a result, the traditional 'tragedy of the commons' framework might be more complicated in the case of OSS. While the classic 'tragedy of the commons' problem – that when everyone benefits from a commons, no one single actor takes action to contribute back[103] [104]– can apply to open source code in its static state, it is much more complicated in the way OSS is produced. Eghbal's dual-level analysis revealed that OSS faces two simultaneous tragedies of the commons: the traditional under-provision problem at the code level (e.g. not enough contributors) and an over-exploitation problem at the production level (e.g. excessive user demands deplete maintainer attention).[105] (This is further

complicated when you consider the differences between end-user applications and services and the types of foundational technologies we are arguing the EU-STF should support.)

This 'dual tragedy of the commons' framework changes how we understand how funding should be structured. Funding approaches that focus only on incentivising more contributors (addressing the under-provision tragedy) may actually worsen the attention depletion tragedy by increasing user demands on already overwhelmed maintainers.[106] Instead, funding mechanisms should prioritise sustainable maintainer capacity – directly supporting core developers, providing administrative infrastructure, and implementing governance tools to manage user demands – rather than simply increasing contributor volume, which could exacerbate the very attention scarcity problems that lead to project abandonment.

The dual tragedy framework also reveals why public-led pooled funding can be important for addressing OSS sustainability challenges. Unlike private funding from software companies – which often ties to specific business needs that may increase maintainer workload through feature requests and support demands – public-led funding (complemented by private contributions) can invest in foundational but unglamorous administrative support, governance tools, and sustainable maintenance practices that benefit the broader digital commons. Public funding mechanisms therefore offer the systemic coordination needed to address attention management across the entire OSS ecosystem.[107]

This does not negate the need for private or volunteer investments, or challenge the benefits market-driven sustainability models have brought forth. Instead, it suggests that new models are needed for conceptualising how a public-led intervention can bring public and private capital together to address these issues in a new and novel way, at the scale of the European economy. Despite significant existing private investment – with organisations contributing approximately USD $1.7 billion annually to OSS projects, primarily through employee time[108] – critical gaps remain because companies naturally direct resources toward projects they recognise as business-critical. This leaves many equally important foundational libraries that benefit multiple organisations without dedicated support, with no single company responsible for maintenance.[109]

As a result, OSS demands a nuanced examination of how it is maintained and produced in order to understand the lack of commensurate investment and the unique benefits of public-led interventions. Even putting this aside, though, there are regular market failures that help explain the lack of investment in open source technologies. For example, it is true that many OSS projects are maintained by employees at large technology firms – an estimated 86% according to Linux Foundation research[110] – but this suggests a limited pool of contribution, when in fact the overall pool of contribution could be much higher if there were diverse forms of investment and support to help fund individual developers and projects.[111]

Libraries which are used in the supply chains of critical infrastructure have strong evidence of under-maintenance (especially as it relates to potential security vulnerabilities).[112] The contribution of private support does not always go towards the projects of strategic interest in digital supply chains, many of which remain under-maintained and therefore under-invested. For example, an analysis of PyPI libraries found that many widely used but smaller dependency libraries suffer from under-maintenance, as vulnerabilities often remain unaddressed due to inactive maintainers and lack of resources,

highlighting the funding gap for critical supply-chain components.[113]

Several broader system failures also provide strong economic justification for future public (and indeed private) support of OSS initiatives. For example, risk-taking challenges, as highlighted by Mariana Mazzucato's work on entrepreneurial states, demonstrate that private markets often under-invest in foundational technologies with uncertain returns.[114] Scaling failures occur due to market indivisibilities, creating classic infant industry arguments for industrial policy intervention. Additionally, positive externalities through learning-by-doing effects and network effects are systematically undervalued by private actors, leading to suboptimal investment levels. This demonstrates a strong rationale for state and public involvement in their provision.[115]

Open source also addresses broader system failures in creating coherent innovation ecosystems. Building such ecosystems requires coordinated efforts that individual market actors cannot achieve independently. This system-level perspective emphasises the need for transformative objectives that align with broader societal goals, and helps us to understand the interrelation between open digital infrastructure investment and competitiveness. This thinking was at the core of the German STF. European policy documents, including the Draghi report, but also the Competitiveness Compass[134] and even the recent 2025 German coalition agreement,[135] increasingly recognise these system-level challenges and propose mission-driven approaches to address them.

An EU-STF offers the right vehicle for internalising and guiding the positive spill-overs of the public goods produced through OSS activity. A public-led intervention which pools public sector and industrial resources can supply the means to secure their maintenance when commercial incentives are not sufficient for long-term provision. The dual tragedies of the commons and these market/system failures demonstrate that focused, well-structured investments in developer resources could be determinative, and an area the public sector can lead on. Guaranteeing the provision of a viable and vibrant open source ecosystem not only facilitates the supply of OSS as a public good, but constitutes a strong asset for Europe.

3.2.2 The economic benefits of OSS investment

The positive economic effects of OSS activities have frequently been underlined. Even relatively small increases of capital injections or state funding for OSS activities can have a significant positive growth effect on par with large scale European investment or research programmes like the Trans-European Transport Network (TEN-T) or Horizon Europe.[116] Furthermore, OSS activities have significant impacts on the economic complexity of countries by increasing country economic diversification. This has the effect of not only reducing the dependence on international suppliers, but increasing the resilience of a country's exports by reducing dependence on specific individual goods and services.[117]

At the same time, a push towards more OSS usage in tech has the potential to boost the establishment of open standards[118] in different industries, lessening the danger of a lock-in on specific vendors of software or hardware. This allows firms (specifically SMEs) to seek out more cost efficient solutions better suited to their business models independent from licensing, thereby reducing the risk to the overall economic supply chains.[119] [120] Therefore, establishing and institutionalising a European means to push for increased development of the OSS economy – as well as the sustainable

use and maintenance of its products – promises significant and tangible benefits regarding economic growth.

Additional to the economic benefits, European digital sovereignty could further profit from the innovative push caused by increased open innovations resulting from OSS development and its associated spillovers.[121] [122] [123]An increase in European commitment to global OSS development and maintenance can cause a strong positive effect on the domestic formation of information technology (IT) start-ups, as well as EU patents and trademarks.[124] This also reduces costs for new business models and technological experimentation, enabled by the ready-made portfolio of transferable knowledge and code available through OSS productsm as well as the strongly interconnected cooperative open source communities centered around their creation.[125] Consequently, any European increase in support for OSS – be it in the shape of an EU-STF or otherwise – should prioritise those aspects of the tech stack which show the greatest need for European industry and offer the highest spillovers; as, for example, in the areas of ODBTs, AI, cybersecurity, or OSH development.

Currently, funding in the open source ecosystem is dominated by a few big players. For example, large foundations like the Linux Foundation,[126] Apache Software Software,[127] or Eclipse Foundation[128] often do a lot of investment on their own, but also have their own specific goals which guide their decision-making, including their mandate to reflect the interests of their members if they are a trade association. Software companies, on the other hand, often have a vested commercial interest aiming to build up markets for complementary services, to increase their innovative capability, or to enable cost reductions through outsourcing to external communities.[129] [130] Evidently, while acknowledging these contributions,[131] these particular interests by private players are not sufficient to facilitate either the long-term sustainability of the open source ecosystem, nor guiding it towards a structure which supports European interests.

To enable individuals and entrepreneurs to invest and innovate in OSS, stronger and more reliable government-provided incentives are needed.[132] If the EU aims to increase its economic growth through OSS, it needs to place itself as a reliable funder, consumer, and supplier of OSS as public good by acting as a market creator where the markets fail to supply. At the same time, given its potential to act as a driver for innovation and positive spillovers through open standards and knowledge creation, any European or national-level intervention needs to be guided towards greater reliability and systemic resilience for the open source ecosystem. Such an approach should aim at reducing the potential negative externalities of cyberattacks and accidents by increasing the security level, in order to justify a higher level of EU involvement.

Intervention of this kind entails the need for publicly provided resources for the long-term maintenance and security of projects. It must also include measures which target start-up investment and capital formation to scale up those open source projects that can become independently sustainable through private-driven development. Such efforts shouldrecognise that many ODBTs lack viable commercialisation pathways and therefore require long-term public investment in their maintenance, akin to other essential infrastructure like roads or bridges.

Any such intervention needs to be flexible and adaptable enough to further, and not stifle, the creativity and innovativeness which is inherent to the open source community. Hence, the EU-STF

needs to be more than a simple funding mechanism and include sufficient domain knowledge. It must be endowed with a strong mandate for targeted, intelligent decision-making, with the goal of creating and supporting an effective European open source innovation ecosystem. A model for this can be found in the example of the German STF, an approach which – if flanked by strong political support (for example through dedicated missions aimed at digitalisation through open source in the new Framework Programme[133] – could lay the foundation for a reinvigorated and strengthened open source ecosystem in Europe.

3.2.3. Mission-driven investment in open source technology

A mission-driven approach to investing in open digital infrastructure must correct these market and system failures. Such approaches demonstrate how a tangible public-led intervention can create a concrete alternative pathway for supporting open source sustainability, maintenance, and security, thereby advancing the policy objectives of digital sovereignty, cybersecurity/cyber resilience, and competitiveness. This approach must emphasise investments in maintenance and security as enabling digital autonomy and digital resilience, creating the preconditions for improved security, innovation, and competition.

Digital autonomy and digital resilience are complementary pillars supporting Europe's broader digital sovereignty objectives, each addressing distinct but interconnected challenges in the contemporary technology landscape. Digital autonomy, sometimes called 'strategic autonomy' in an EU context, focuses on reducing external dependencies and maintaining strategic control over critical technologies. This enables Europe to make independent choices and decisions about its digital future without being constrained or coerced by foreign technological gatekeepers or other geopolitical pressures.[136] On the other hand, digital resilience, sometimes called 'cyber resilience' in a cybersecurity context, emphasises the capacity to withstand, adapt to, and recover from technological disruptions, cyber threats, and supply chain failures that could compromise essential digital services and infrastructure.[137]

Investment in open source technologies uniquely advances both objectives – autonomy and resilience – by creating secure and sustainable open assets that are neither influenced in large part by external actors nor vulnerable to single points of failure. Open source technologies can support digital autonomy by ensuring that core software, algorithms, and standards remain accessible and modifiable by European entities rather than being locked within proprietary systems controlled by foreign corporations. Simultaneously, these technologies enhance digital resilience and competition through their distributed development model, transparent security practices, and community-driven maintenance that reduces the risk of vendor lock-in, supply chain manipulation, or sudden service discontinuation.

This dual benefit makes open source maintenance investment a strategic multiplier for digital sovereignty goals. By enabling autonomy and resilience, Europe can build technological capabilities that are both independent and robust, positioning the continent to navigate an increasingly complex and contested digital geopolitical environment while maintaining the flexibility to adapt its technological trajectory according to its own values and interests. Digital sovereignty is not about geopolitical competition and isolationism, it is instead about autonomous, self-determined use of technology that

allows governments to have more choice by giving them credible alternatives to switch to. Openness enables the autonomy and resilience that makes digital sovereignty possible. Investing in open source sustainability, maintenance, and security instead addresses critical market and system failures that hinder optimal technological progress.

Cybersecurity is a central pillar of this vision of digital sovereignty. Open source, when properly maintained and secured, offers a level of transparency and collective oversight that proprietary systems cannot match, enabling faster identification and remediation of vulnerabilities. However, the current over-reliance on a small number of underfunded maintainers for critical open source components introduces supply chain risks for both the public sector and industry. Investing in the security and long-term maintenance of ODBTs directly mitigates these risks by strengthening the integrity of global software supply chains for digital technologies.

Open source is also inherently in the interest of the challenger, and Europe are in many ways the challengers given American and Chinese tech dominance. Rather than competing on the terms set by incumbents, Europe should embrace open source and open standards, making it more digitally competitive. Investing in ODBTs would reduce barriers to entry, increase interoperability, and foster collaboration across borders. In this way, investing in open source is not just a tool of governance or ideology, but a pragmatic strategy for regaining technological leverage in a world where the dominant platforms were not made in Europe.

Here the importance of global open source collaboration must be stressed, and the fact that digital innovation thrives in collaborative environments where knowledge sharing accelerates development. Europe wins by strengthening the global commons that allow people to be autonomous (e.g. have choice) and be resilient (e.g. bounce back) in markets that promote consolidation and have long been fine with the status quo. Its sovereignty, security, innovation capacities, and competitiveness therefore do not come at the expense of creating more fragmentation in digital collaboration globally.

IV. From Proposed Benefits towards an Implementation of the EU-STF

We will now discuss how to begin moving from proposed benefits towards an implementation of a mission-driven EU-STF. There is a lot to learn from the model of the German STF and the modern German Sovereign Tech Agency, which is of huge relevance for the design and setup of an EU-STF that fulfils some of the broad objectives highlighted above. Understanding these precedents helps provide understanding of different points of emphasis necessary for the development and articulation of the EU-STF, and is a precondition for considering how it will be funded and implemented – and on what legal basis. (The latter will be covered in Section V.)

4.1. Precedents for the Establishment of an EU-STF

Section 4.1 briefly surveys some of the key instruments – drawn from both the US and Europe – that provide useful precedents for open source or digital innovation funding that might be expanded on by the EU-STF. That being said, no funding on the order of what the EU-STF is proposing has been attempted at the EU level, meaning the comparison is an imperfect one. These differences will be noted under each of the examples.

4.1.1. Next Generation Internet

The EU has established several significant initiatives supporting OSS and related digital technologies, some of which offer hopeful precedents for a mission-oriented EU-STF. The Next Generation Internet (NGI) Initiative,[138] launched by the EC, represents the most substantial commitment to open internet technologies, allocating EUR €140 million between 2019 and 2024 across over 1,200 projects,[139] with an additional EUR €32 million planned for 2024-2027.[140]

Central to NGI is the cascade funding model (e.g financial support for third parties), which enables public funds to reach startups, SMEs, and other third parties through intermediary organizations. Cascade funding is also known as Financial Support to Third Parties (FSTP), a mechanism launched under Horizon 2020 and continued under Horizon Europe[141] to distribute public funds to startups, SMEs, and other innovators via intermediary consortia.[142] It simplifies access to EU funding by allowing large projects to issue open calls and offer smaller, equity-free grants directly to third parties. It has been most widely used in the NGI initiative, supporting a distributed and accessible approach to digital innovation funding through the NGI Open Calls), which has substantially reduced the burden for applying to and reporting on funding for individuals, communities, and SMEs.

In comparison to the NGI, the EU-STF would be a proposed strategic investment instrument focused on long-term resilience and security of foundational open source digital infrastructure critical to Europe's digital sovereignty. The NGI emphasises experimentation and decentralised innovation – an approach common in EU digital policy generally, including in the recent leaked draft of the FP10, establishing Horizon Europe (2028 - 2034), such as its Pillar 4 on the European Research Area including 'research and innovation infrastructures'.[143] Meanwhile, the EU-STF would prioritise maintenance, scale,

and sustainability of core technologies. In other words, the focus would be much more on maintenance of ODBTs than on innovation, even though the EU-STF's support for core development and maintenance of open digital infrastructure would provide the basis for open innovation as a positive externality. Additionally, NGI operates as a research programme underneath the Horizon Europe programme, whereas the EU-STF would function more like a mission-driven instrument for funding open digital infrastructure.

4.1.2. EU Free and Open Source Software Auditing and EC-OSPO Funding

Representing its first foray into addressing open source vulnerabilities – triggered by the HeartBleed cybersecurity crisis – the EC allocated much welcomed initial funding for OSS and OSS components beginning in the 2010s. This included EUR €1 million in 2014 to a bug bounty programme called EU Free and Open Source Software Auditing (EU-FOSSA) (2014 – 2016) and EUR €850,000 to EU Free and Open Source Software Auditing 2 (EU-FOSSA-2) (2017 – 2020), both managed under the Directorate-General for Digital Service (DG-DIGIT). Continuing that legacy, in 2021-2022, the EC's Open Source Programme Office (EC-OSPO) (which itself launched in 2020) began a similar programme.[144] Although those projects were rightly lauded as important and popular,[145] their scope was mostly limited to bug bounties and OSS widely used by EU institutions. Experts have observed that while bug bounties may enhance OSS security for mature projects when carefully implemented and under certain circumstances, funding approaches that pair targeted security and maintenance funding – such as the EU-STF's model – are preferable.[146]

4.1.3. Joint European Disruptive Initiative

Beyond open source-specific programmes, the Joint European Disruptive Initiative (JEDI) provides funding for breakthrough technologies across multiple sectors, including digital technologies, environment, and health.[147] JEDI is a pan-European, US Defense Advanced Research Projects Agency (DARPA)-inspired agency that funds 'Technology Grand Challenges' across sectors including digital, environment, health, education, oceans, and space to boost Europe's position in breakthrough technologies. It supports over 6,000 researchers in 29 countries, using a foresight-driven method focused on speed, excellence, interdisciplinarity, and bold risk-taking.[148] This broader innovation funding landscape aims to position Europe as a leader in emerging and disruptive technologies, while maintaining its commitment to open and collaborative approaches.

In the broader European innovation funding landscape, JEDI represents a complementary model to open source–specific programmes like NGI. JEDI focuses on high-risk, high-reward 'moonshot' projects across digital, environmental, and health domains, aiming to enhance Europe's digital sovereignty and global competitiveness. While JEDI's approach is sector-agnostic and centred on radical innovation, it shares with the EU-STF a commitment to strategic autonomy and long-term resilience. That said, the EU-STF would serve a distinct but complementary role. Unlike JEDI, which is focused on future-oriented breakthroughs, the EU-STF is concerned with the sustainability, maintenance, and security of existing foundational digital infrastructure – particularly OSS components that underpin critical systems.

4.1.4. European Digital Infrastructure Consortia

There are other hybrid/shared management structures or models available for supporting novel forms of investment into technology, such as the European Digital Infrastructure Consortium (EDIC). The EDIC is a novel legal framework for pooling Member State contributions to digital infrastructure projects along a common theme,[149] with the pending Digital Commons EDIC offering a promising model for investing in open technologies.[150] The Digital Commons EDIC is a new legal consortium – proposed by France, Germany, Italy and the Netherlands and awaits the EC's approval – that aims to support the development, maintenance, and scaling of digital commons as critical, sovereign European public infrastructure through multi-country collaboration and pooled resources. (More information on the EDIC model – and other similar models – will be detailed in Section V.)

4.1.5. Open Technology Fund

In the US, the Open Technology Fund (OTF),[151] based in the US, provides a valuable reference point for designing public funding mechanisms for open source. While operating in a completely different policy and budgetary context – the fund is focused more narrowly on the topic of Internet freedom within repressive contexts – the OTF has pioneered key practices that lower barriers to participation for smaller projects, such as lightweight and developer-friendly application processes that take account of the limited administrative capacity of most OSS maintainers.[152] Crucially, the OTF has also built strong trust with the Internet freedom community despite its U.S. government funding – an important reminder that any EU-STF must be designed in a way that earns the confidence of the open source ecosystem.[153] Acknowledging the OTF's experience would reinforce broader efforts to create the infrastructural conditions for a truly inclusive and sustainable open source ecosystem, ensuring that smaller actors – and not just large, well-resourced players – can benefit.

4.1.6. Open Source Technology Improvement Fund

The Open Source Technology Improvement Fund (OSTIF)[154] offers a compelling model for how targeted funding can directly strengthen the security and maintenance of critical open source technologies from a security perspective. OSTIF functions as an independent, non-profit intermediary that connects open source maintainers with experienced security auditors and coordinates end-to-end reviews, from identifying vulnerabilities to overseeing their remediation.[155] OSTIF has conducted over 100 security audits, identifying and helping to remediate more than 135 high- and critical-severity vulnerabilities, while also improving testing regimens and directly assisting maintainers with long-term upkeep.[156] Crucially, OSTIF demonstrates that funding alone is insufficient unless paired with independent, expert security resources that work closely with maintainers to implement improvements in a non-disruptive way. The EU-STF could amplify its impact by supporting such specialised organisations and ensuring that maintainers have structured access to expert security support, complementing broader ecosystem initiatives led by larger foundations. This approach would bridge the critical gap between funding availability and tangible security outcomes, ensuring that Europe's investments translate into measurable improvements in open source resilience and digital sovereignty.

4.2. Insights and Learnings from the German STF

The German STF operates with a focused but impactful mandate to support the maintenance of the infrastructure we do not see, but that we rely on – namely ODBTs. In a nutshell, what the German STF does is to pay maintainers to maintain open source, with a strong focus on ODBTs. It is often as simple as those maintainers doing the work, and invoicing the Sovereign Tech Agency GmbH for it. This is frequently done through an open application platform and complemented by active scouting from STF staff, improving the ability of smaller open source projects to get recognised and access the support they need to do their work (much of which goes unrecognised but has significant and widespread applications). While the process might not be quite as simple at the EU level, the goal will be to get as close as possible, in line with the development and collaboration models undergirding OSS development in the 21st century.

The German STF has adopted a formative conception of digital sovereignty in relation to open source technology. It adopts a conception of digital sovereignty defined as: '.. the self-determined use of digital technologies and systems by individuals, industry, and governments'.[157] This understanding moves beyond a narrowly national or protectionist approach. In operational terms, STF beneficiaries are not required to be German citizens, residents, or businesses; funding is available to projects globally. This approach is highly relevant for the design of an EU-STF, as it suggests that maximising impact on European digital sovereignty will depend on supporting the global open source components that underpin Europe's digital infrastructure, rather than restricting eligibility to European-based projects.

The German STF has a remarkable mandate. At the moment, it manages approximately EUR €20 million in 2025,[158] having supported 60 funded projects with timelines ranging from 6 to 24 months.[159] With a team of almost 20 people, the fund demonstrates how targeted public investment can effectively support critical digital infrastructure. The institution runs several programmes, including direct funding for maintenance and security improvements, but also fellowship programmes for individual maintainers and challenge-based initiatives.

The institution has funded many impactful ODBTs over the years. Examples include libraries for programming languages, package managers, open implementations of communication protocols, administration tools for developers, digital encryption technologies, and more. The funding is described as time-limited and targeted at specific challenges or security vulnerabilities. The fund's portfolio demonstrates a strategic focus on infrastructure components that are widely used but often under-resourced. Recent funding decisions illustrate this approach. For example, the organisation has handed SerNet[160] EUR €688,800 to improve Samba, the OSS stack for networking with Windows computers.[161] Similarly, the fund has invested substantially in FreeBSD162 infrastructure projects, recognising the operating system's importance to enterprise and internet infrastructure. Despite the success of these projects, the time-limited nature of this funding model highlights a potential shortcoming that an EU-STF could address by providing sustained, long-term support for critical infrastructure components that lack viable business models and require ongoing maintenance to remain secure and reliable.

The German STF's strategy broadly falls into three distinct project categories that address different aspects of the open source technology lifecycle.[163] Development projects focus on supporting the ongoing development of open source solutions, maintenance projects ensure the long-term

sustainability of open digital infrastructure, and improvement projects enhance existing technologies to meet evolving needs. This comprehensive approach is exemplified by supported projects such as OpenBLAS,[164] which provides essential linear algebra calculations for scientific programming languages; the OpenJS Foundation,[165] which maintains critical JavaScript ecosystem components like Node.js and jQuery; and FFmpeg,[166] a multimedia framework that enables widespread media processing capabilities across platforms.

The institution's portfolio demonstrates the critical importance of foundational technologies that often lack adequate commercial funding. Projects like the Yocto Project[167] – which provides tools for custom Linux-based embedded systems – represent infrastructure components essential for digital sovereignty that are challenging to monetise through traditional market mechanisms. Similarly, support for GNU Network Object Model Environment (GNOME)'s[168] desktop environment reflects recognition that open source technologies require sustained development to compete with proprietary alternatives and maintain technological choice in digital ecosystems.

Beyond direct funding, the STF is integrated in the Sovereign Tech Agency, which provides advisory services and collects knowledge on open source and digital technologies. This holistic approach positions the agency as more than a funding mechanism. It becomes a strategic knowledge hub that can network effectively with countries and coordinate European-level initiatives. The potential for replicating this model at the European level, possibly through institutions like the European Innovation Council (EIC), while coordinating with the German STF presents an opportunity to scale these benefits across the continent while addressing the need for coordinated support of critical digital infrastructure that transcends national boundaries.

4.3. Design Considerations for an EU-STF

The German STF's model offers several insights relevant to the development of an EU-wide equivalent. The fund's demonstrated ability to scale funding from EUR €13 million to nearly EUR €20 million in just two years suggests that appetite for this type of infrastructure investment exists, is reasonable and commensurate, can grow rapidly, and is politically defensible. The scale of demand for funding from the German STF far exceeds its current budget, with nearly 500 submissions requesting over EUR €114 million in funding since applications opened, underscoring the urgent need for greater support for critical open digital infrastructure.[169] The diversity of projects funded – from cryptographic libraries to networking protocols to software development tools – indicates that an EU-wide fund would have no shortage of open digital infrastructure requiring support. Furthermore, the fund's evolution from a fund to a comprehensive agency with multiple complementary programmes suggests that any EU-wide initiative should be designed with similar flexibility and scope for expansion.

It should be noted that the funding needed for such a body is modest compared to the sum total of digital and R&D investment in Europe. Put more concretely, a proposed budget of at least EUR €350 million over a seven-year period (more on the rationale for this number in Section 4.4) is modest when compared to other EU initiatives and the funding they include in the last MFF cycle. This includes a total funding size of EUR €7.5 billion allocated for DIGITAL,[170] a total funding size of EUR €95.5 billion Horizon Europe framework,[171] and even the EUR €43 billion EU Chips Act.[172] These numbers demonstrate that strategic investment at the modest scale of the proposed EU-STF is both feasible and urgently needed.

The focus of the EU-STF should be on both technological and human sustainability, supporting not just code but investment in the labour markets for software development and software supply chains. To put it another way, investing in the human capacity at the core of modern software development – by enabling experienced open source contributors and maintainers to devote sustained time and expertise to critical projects without burning out – will not only strengthen the resilience of Europe's infrastucture, but also create spillover benefits for the European labour market by deepening the pool of highly skilled open source developers working on these technologies full time. As a result, the primary objective of the EU-STF would be to invest in the people and projects ensure the long-term sustainability, security, and support of OSS components that are widely used in European public services, industries, and critical infrastructure, in recognition of the global nature of open source collaboration.

The EU-STF should broadly expand on the key activities of the German STF, with some notional positioning more towards specific EU dependencies on OSS and OSS components which are part of critical digital infrastructure. Given the scale of this challenge, we argue that the potential EU scale means that it must be a matter of industrial policy. The EU-STF should be led by public policy as a public-private partnership, with strong emphasis on values- and standards-setting. This requires the EU to both invest itself, as well as act as a leader that can incentivise private sector investments in open digital infrastructure, in line with its competitiveness goals.

Additionally, given the criticality of both public and industrial infrastructures, the EU-STF must engage critically with narratives, frameworks, and legislation around cybersecurity. While the German STF has engaged with the security aspect of its work through its Sovereign Tech Resilience programme,173 it has not so explicitly aligned its mission with coordination with regulatory requirements, particularly those brought in in recent months by the EU CRA.174 European security and software supply chain issues are currently of huge importance. Security-focused investments must be a critical element of the work of the EU-STF and be baked into the logic of the fund's model for how and what it invests in.

4.4. Implementation Considerations for an EU-STF

The EU-STF must be designed as an agile and non-bureaucratic institution, capable of supporting fast-evolving technical communities, responding to urgent vulnerabilities, and making targeted, iterative investments in open digital infrastructure. By combining funding capabilities with deep technical expertise and real-time market and ecosystem intelligence, the EU-STF can actively shape European technology strategy while coordinating investments that serve long-term objectives of security, innovation, autonomy, resilience, and competitiveness.

4.4.1. Justified size of budget for the EU-STF

Determining an appropriate source of funding and commensurate levels for an EU-STF requires a nuanced understanding of different project types and their distinct needs — often, but not always, financial. A critical distinction should be made between 'development' and 'improvement' projects that demonstrate potential for private sector integration and commercialisation, versus 'maintenance' projects that provide high strategic importance and economic returns. but which are harder to quantify the value of and therefore commercialise. This fundamental difference in commercial viability directly

impacts both the extent and duration of necessary public funding, with maintenance projects potentially requiring long-term institutional support rather than time-limited funding.

A first attempt to discuss the funding of an EU-STF is based on scaling up the funding amount of the German STF, which reflects the level of investment the German government has already made rather than the actual funding needed. The German STF has supported 60 projects in three years. The average project weighted by project duration received a funding of around EUR €450.000, so the funding of the German STF in three years is around EUR €27 million. Scaling this funding up to the EU level by population, where Germany represents around 19% of the EU population, this results in a funding of around EUR €146 million in three years. For a seven-year period, this means around EUR €341 million.

We propose a base level of EUR €350 million to consider not only inflation, but also to suggest a round number for the EU-STF funding. This should be understood as a lower bound, given that EUR €50 million per year would not even cover the unsolicited funding requests the STF receives today. The total amount can and should be further increased through member state and industry co-financing. That said, based on the experience of the German STF, an EU-STF will do more than just funding, if it follows a mission-driven approach.

The German STF formulated a clear directionality and agenda for its funding activity, which results from a deep knowledge of and exchange with the ecosystem. The German STF serves as a fast address for policy makers to get informed on specific challenges within the open source ecosystem or digitalisation, in general, including the question of digital sovereignty. In that way, a mission-driven EU-STF is effectively tackling the demanding requirements of digital transformation. Such a mission-driven vehicle should be equipped with expertise in specific thematic areas and possess the autonomy to operate within the scope of its competencies and assume a prominent role vis-à-vis the EU administrative system, including linkages to EU actors.

4.4.2. Core activities of the EU-STF

To direct this funding towards adequate impact, this study found that the EU-STF should focus on five core actions. These include:

Action #1: Mapping and Identifying OSS Dependencies and Projects of Strategic Interest

The first step to ensuring the EU-wide relevance of the EU-STF is to comprehensively map out the software dependencies used across critical infrastructure and public services within the EU. This should be done in order to understand which ones are vulnerable to issues in sustainability and issues related to maintenance, or security issues related to vulnerabilities, malicious intent, or social engineering. By understanding where dependencies lie, the EU can better assess potential vulnerabilities and reduce risks associated with supply chain attacks, under-funded or under-maintained software, or foreign influence over crucial software components. The EU-STF could directly complement and support CRA implementation by funding targeted maintenance and security improvements for the most critical and under-resourced dependencies identified through this process.[175] It can also better prioritise foundational components which support common projects of

strategic interest for industry and the public sector, or which advance critical EU development and security objectives.

Action #2: Investing in Maintenance

For OSS dependencies and projects of strategic interest found to have maintenance issues, the EU-STF should strategically invest in their ongoing maintenance by investing directly in their maintainers or core developers, irrespective of their countries of residency. This support would bolster their ability to do any number of essential activities, including (but not limited to): buying development time, developing patches, and creating project improvements or updates. By investing in the core sustainability of the developers behind the code, the EU ensures those vital projects remain supported, strengthening the open source technologies behind proprietary and open source applications, services, and infrastructure alike. Project identification and investment must be done in close coordination with the open source community.

Central to this approach is the use of a public procurement model rather than traditional grant-making mechanisms. The EU-STF would procure maintainers and core developers to perform essential maintenance and development work on their projects, creating a contractual relationship that ensures accountability and deliverables while respecting the autonomy of open source communities. This procurement approach recognises that maintaining open source infrastructure is legitimate, valuable work that deserves professional compensation and clear project outcomes. By procuring services rather than awarding grants, the EU-STF can establish clear expectations for deliverables, timelines, and quality standards while maintaining the flexibility needed to work within the diverse governance structures of different open source projects. This model has proven effective in the German STF experience and represents a more sustainable and professional approach to supporting critical digital infrastructure than ad-hoc funding mechanisms.

Action #3: Investing in Security

For dependencies found to have security issues, rigorous security audits must be conducted to assess their integrity, security posture, and overall resilience against cyber threats. These audits should not only involve code reviews, vulnerability testing, and support for compliance with international and EU cybersecurity standards but also provide direct access to specialised security expertise for maintainers who often lack in-house capacity or formal cybersecurity training. Open source projects cannot simply 'become secure' through funding alone; targeted security uplift requires close collaboration between maintainers and experienced security organisations. This would also require dedicated staff who can embed in projects and understand the real security challenges they are facing as it relates to how they are being run, in line with the OSTIF model for auditing.[176]

The EU-STF should therefore be designed to work directly with maintainers to procure independent security resources through trusted intermediaries already active and successful in this field. This could include, for example: the OSTIF for rigorous security audits and code reviews;[177] which through LF Security and its training programmes (e.g., Kubernetes Security Fundamentals, Security for Software Development Managers) equips developers with practical cybersecurity skills;[178] and the Eclipse Foundation, whose Project Security Incident Response Team (PSIRT) and Rapid Security Reviews

initiative provide structured, accessible assessments and remediation support for OSS maintainers.[179] These initiatives have proven their effectiveness but require substantially more funding to operate at the scale needed to address open source security maintenance as a systemic issue. By coupling funding with these tangible, expert-driven interventions, the EU can ensure that security assessments translate into actionable improvements, mitigating risks proactively while supporting maintainers.

Action #4: Investing in Improvement

The EU-STF should maintain improvement projects as a distinct funding category alongside maintenance and security, rather than treating it as a subset of either. Unlike maintenance, which focuses on sustaining existing functionality, or security, which addresses vulnerabilities and resilience, improvement projects are about enabling already trusted and widely used technologies to take the next step in their development – such as scaling to higher user numbers or expanding critical functionality.[180] This category is essential to ensure that open digital infrastructure not only remains secure and stable but also evolves to meet growing EU-wide demand, particularly for strategically relevant components.

The emphasis should be on investing in capabilities that enhance core functionality and ensure the long-term viability of critical infrastructure projects, rather than feature creep or competitive productisation. Priorities for such funding should be determined in consultation with projects identified through the dependency mapping and strategic prioritisation steps. While this differs somewhat from the German STF's heavier emphasis on maintenance and security, it reflects the EU-STF's broader policy objective of strengthening open source as a pillar of Europe's digital sovereignty and ensuring strategic scaling where relevant.

Action #5: Investing in Ecosystem-Strengthening Activities

To strengthen the open source ecosystem, the EU-STF should be responsible for coordinating with various stakeholders in the open source ecosystem. This should include public authorities, members of industry, maintainers/developers, and intermediaries (e.g. community organisations, OSS Stewards under the CRA). Engaging with these actors will help align efforts, share intelligence, and enhance cross-border cooperation, ensuring a unified approach to sustaining and securing critical digital infrastructure. Such investment also helps ensure that other investments and funding are not duplicated, in coordination with other open source and digital policy funders. It should also foster collaboration between these stakeholders to create sustainable support networks, facilitate knowledge exchange and seek to match public and private funding. Additionally, the EU-STF should develop training programmes to equip maintainers and developers with secure coding practices and vulnerability management skills, as well as peer-support programmes to strengthen social cohesion and personal contacts in the open source community.

More broadly, the German STF has successfully demonstrated that public funding can be effectively structured to support critical open source projects while maintaining operational flexibility and building community trust. These elements should carry over to the EU-STF. Key elements of the this approach should be (for example):

- Developing a One-Stop-Shop funding approach that minimises administrative burden for OSS maintainers, including during the funding application/project scouting process, and ensures that financial support is distributed efficiently and transparently.

- Implementing an open and participatory selection process for identifying high-impact OSS projects that need support, ensuring that the fund responds to real security and sustainability challenges in the ecosystem.

- Building in balance between proactive and reactive funding to allow for both long-term investment in critical OSS infrastructure and rapid response to emerging security risks.

- An international funding scope which stipulates the funding need not be limited to EU entities (e.g. individual's organisation), but should instead be chosen based on identified needs and dependencies in Europe.

4.4.3. Design criteria for the EU-STF

Across these discussions, broad consensus emerged that many EU funding schemes are often too rigid, slow, or misaligned with how open source ecosystems operate.[181] Interviewees consistently emphasised the need for agility, reduced administrative burden, and meaningful collaboration with the ecosystem. Broadly, they highlighted that any successful fund must be tailored to the unique governance, incentive structures, and maintenance dynamics of OSS. In other words: the logic for the fund must ensure that money goes to recipients who deliver the best work, not recipients who write the best applications.
These insights shaped the design criteria proposed for the EU-STF. The criteria are as follows (and will be expanded on more in the next section):

1. Pooled Financing and Coordination: The EU-STF should enable joint investment from the EU, Member States, and industry to consolidate fragmented efforts and ensure strategic alignment across borders.

2. Low Bureaucracy: To remain attractive and accessible to open source communities, the EU-STF must minimise bureaucratic overhead and simplify compliance processes.

3. Political Independence: The fund should operate with institutional autonomy and multistakeholder input to ensure decisions reflect both public priorities and the needs of the open source ecosystem.

4. Flexible Funding: It must support a range of funding models – including microgrants, emergency response, and long-term core maintenance – while maintaining proportionate oversight mechanisms and ensuring flexibility in funding recipients.[182]

5. Community Focus: The EU-STF should embed structured collaboration with open source communities, foundations, and industry to co-define funding priorities and respond to evolving needs.

6. Strategic Alignment: All funding decisions must be grounded in EU policy goals – such as digital sovereignty, cybersecurity/cyber resilience, and competitiveness – and compliant with state aid and procurement rules.

7. Transparency: The fund must uphold transparency in governance, funding allocations, and evaluation metrics to foster trust and legitimacy across stakeholders.

V. Detailed Governance Setup Evaluation: Implementing and Governing the EU-STF

This section explores in-depth the feasibility of specific governance setups and funding sources for the EU-STF. Keeping in mind the scope, complexity, and urgency of the current political moment, we recommend options that rise to the scale of the challenge while being expedient and implementable. In particular, a novel governance setup is necessitated because of the requirement of very low barriers to access funding for maintainers specific to open source maintenance, as does consideration of needs such as pooled financing, low bureaucracy, and political independence.

In evaluating different legal, governance and funding options, it is important to consider how these two dimensions – ambition and urgency – interact. For example, in standalone models, or when embedding the instrument into existing EU programmes, governance and funding are inherently linked: either a new structure is created alongside dedicated funding, or existing instruments come with established governance and budgetary rules. Hybrid models – such as Joint Undertakings (JUs), Important Projects of Common European Interest (IPCEIs) or EDICs – or decentralised frameworks, by contrast, offer governance models designed to aggregate and coordinate funding from multiple sources, including the EU, Member States, and private actors.

In the following sub-sections, we will survey the legal feasibility of different options for the EU-STF, which informs our later recommendation of an EDIC as the preferred model (in Section VI). We survey each of the categories of setup that was considered and provide the background and context that will help explain our later evaluation of two categories of setup in particular (Section 5.1). We then analyse the rationale for two preferred categories of governance setup, including the advantages, disadvantages, and trade-offs of those broad categories and specific models within them (Section 5.2). This analysis has been done based on seven criteria above Finally, we explain how the set up of EU-wide funding structures for open digital infrastructure will mean creating corresponding tools for coordination (Section 5.3), as well as explore implementation considerations for each category that might inform the determination of the most pragmatic approach by policymakers (Section 5.4).

5.1. Overview of Institutional Setup Categories

The design and implementation of the EU-STF must balance political feasibility, operational flexibility, and strategic impact. This section outlines four institutional setup categories, each with distinct advantages, challenges, and trade-offs.

5.1.1. Standalone and centralised fund

A standalone and centralised EU-wide fund represents the most institutionally ambitious model. This approach would involve the creation of a dedicated legal mandate set out in legislation, as well as a budget line allocated via the MFF negotiation process. Such a fund could be directly established by the EC (possibly coordinated through a Directorate-General (DG) like DG-CNECT). This would likely facilitate lower levels of institutional independence, although an option – that would preserve some level of

political independence – is to leave the executive part to an EU executive agency or to a new body with strategic oversight, rather than have it managed by an existing DG. New legislation offers the opportunity to design the fund in accordance with the criteria and considerations we will highlight in Section 5.2.

A DG could administer funds for a centralised fund, most likely DG CNECT, with the executive part left to an existing executive agency (most likely, HaDEA).[183] Alternatively, DG CNET could delegate the executive part to a new agency, potentially called the European Digital Infrastructure Executive Agency (EDIEA) (as an illustrative name). In the former case, the EC would directly govern the EU-STF, with DG-CNECT playing the lead role in defining priorities, approving funding decisions, and managing overall implementation. This model would ensure close alignment with EU digital policy goals and enable strong political oversight. However, it would likely lack institutional independence and face highly exposure to shifting political priorities, risking slower decision-making and reduced agility in responding to fast-moving digital infrastructure needs. In this context, it is worth considering existing EC implementation structures that could support aspects of the EU-STF, especially in its early stages. The European Health and Digital Executive Agency (HaDEA) is one such example of the EC's executive agencies taking responsibility for implementing parts of key funding programmes like DIGITAL, EU4Health, Horizon Europe, and CEF.

In the latter case, the EC could still retain strategic control via DG-CNECT), but delegate most of the operational and administrative functions to a newly created executive agency or other funding vehicle. This may preserve some separation between political oversight and fund administration, leveraging the agency's purpose-built capacity to manage and disperse digital and infrastructure funds. While this setup could take considerable time and effort to become operational, it could reduce administrative burden in the long-term, avoiding standardised administrative procedures and structures that often weaken ties to the open source community that could limit the fund's flexibility and community focus. Through purposive legislative design, it could become operational in a way that significantly departs from past models, building on precedents such as the NGI programme.

A key advantage of such a centralised model lies in its coherence and the strong political signal it sends. This would include a shared vision for EU digital sovereignty, a commitment to cybersecurity/ cyber resilience, and alignment with other EU policy. Furthermore, such a model would avoid mission drift, ensuring that the EU-STF remains focused on its core objectives. It also allows for more direct oversight of strategic investments in critical open digital infrastructure. That said, setting up and governing a centralised fund presents several challenges.

At the outset, establishing such a fund is very time intensive and partly depends on the political will necessary to prioritise open digital infrastructure investment. Over time, it would be subject to more political scrutiny, centralisation risks administrative inertia, and the lengthy legal and institutional setup process may delay implementation significantly. This might lead to less transparency and political independence, potentially undermining the urgency of Europe's digital policy goals. Establishing a centralised EU-STF would likely fall under the next MFF, as the time required for the adoption of the relevant legislation and its institutional set-up makes its implementation before that highly unlikely. While this longer timeline may be seen as a constraint, it would also avoid conflicts with the current MFF allocations beginning in July 2025 and enable consideration of how the next MFF could support such an investment in critical digital infrastructure. However, this would ultimately depend on whether the next

MFF is designed to explicitly accommodate long-term, non-commercial digital infrastructure funding, potentially requiring new budget lines or adjustments to existing programmes to set the EDIC up for success.

The fund, while standalone, needs to be closely linked to the open source community, which ultimately maintains software as digital infrastructure. Such alignment is crucial to ensure that funds are distributed effectively in response to concrete needs of open source development and maintenance. To avoid misalignment and missteps, community input should be sought throughout the legislative process (not just during proposal development). Developing innovative avenues for their involvement could help.

In the current budgetary context, securing the necessary level of funding at the EU level may prove challenging, particularly in the initial phases. However, a centralised fund that requires a legal act to be set up would almost certainly be funded under the next MFF, starting in 2028, simply because it would take that long to adopt the legal act and create the new institution. While that relative slowness is a disadvantage, it would avoid many of the institutional challenges outlined here, because the new MFF is not allocated yet; on the contrary, the negotiations are just starting and the first legal acts are just about to be proposed in July and September. All the programmes that directorates like DG-CNECT, DG-DIGIT and DG-GROW are already committed to are under the current MFF, not the upcoming one, meaning a centralised funding mechanism would not necessarily create institutional overlaps or stretch administrative capacities.

5.1.2. Embedded or integrated funding

Given the objectives of the EU-STF, which align with existing EU programmes and funding mechanisms, it could be a good choice to embed it into that framework. This has the advantage of aligning resources and ensuring complementarity with other ongoing EU initiatives. More specifically, this approach would involve allocating a distinct operational and financial stream within the framework of ongoing funding programmes such as CEF Digital[184] and DIGITAL[185], or other relevant instruments, including the European Cybersecurity Competence Centre and Network (ECCC).[186]

Rather than establishing that standalone governance entity detailed above, this model aims to build on what already exists. It might do this by embedding the EU-STF into institutional frameworks that are already operational, therefore leveraging existing capabilities in terms of financial management, as well as operational and programme delivery processes. The main strength of this approach is its ability to accelerate implementation while ensuring strategic coherence. Indeed, given the relatively limited budget initially foreseen for the EU-STF, leveraging existing programmes such as CEF Digital and DIGITAL – which present well-established funding instruments, clear procedural frameworks, and an experienced executive agency (namely, the already-mentioned HaDEA)187 – would allow for a rapid and effective setup of EU-STF interventions. Furthermore, this integration would prevent institutional overlaps, avoid the creation of redundant administrative layers and enhance the overall alignment of the EU-STF with the EU digital policy ecosystem.

In practice, this model would likely encounter significant limitations and complications. Embedding the EU-STF within broader, multi-purpose programmes, which address multiple priorities in the digital

realm, may lose its strategic focus and visibility. There is a concrete risk that the EU-STF's specific objectives may be diluted. Indeed, its long-term policy impact could be compromised if the fund is perceived only as a secondary component rather than as an autonomous strategic initiative. Additionally, it would require coordination with existing programmes of work, perhaps diluting its focus, and embedding it into those programmes might require a legislative amendment (such as to the CSA to update ENISA's mandate).

Furthermore, aligning the EU-STF's mandate with existing programmes may introduce institutional hurdles. This potentially limits its capacity for agile responses to evolving threats that require rapid action – a key element for the EU-STF's effectiveness. For example, the DIGITAL programme requires that funding only be disbursed to legal entities established in Europe or associated countries (Art. 18(1) Digital Europe Regulation), which would likely exclude many open source maintainers globally who work on critical digital infrastructure upon which Europe depends. Additionally, the governance architecture of current funding instruments may not fully meet the concrete operational demands of the EU-STF, particularly in areas that require rapid resource mobilisation, continuous maintenance, and the involvement of a plurality of stakeholders.

5.1.3. Hybrid/shared management structure or coordination model

A hybrid or shared management structure – such as a network of local, national or regional nodes coordinated by a central EU entity – seeks to combine EU-level funding and strategic direction with Member State and industry co-investment. Mechanisms like JUs, IPCEIs or EDICs are possible legal frameworks for this setup. All three are instruments for implementing 'multi-country projects' (MCPs). MCPs are large scale projects facilitating achievement of the digital targets under Article 4 of Decision 2022/2481 for the Digital Decade Policy Programme 2030 (DDPP Decision).[188]

These vehicles share several key characteristics. This includes their ability to 'enable large-scale projects that one single Member State could not develop on its own; pool resources to achieve economies of scale and increase impact, and build ecosystems of excellence big enough to attract and retain talent'.[189] The shared model aligns with calls for distributed governance and greater participation of industrial players, while still ensuring the concrete involvement of the EU. It could enable coordinated but diverse investments and help pool resources which align with the strategic objectives of the EU-STF.

This model is perhaps the most politically viable and operationally flexible option. This is especially true with regards to scaling investments and aligning with national cybersecurity agencies, industry priorities, and EU-wide strategic goals. Its flexibility and distinct legal nature makes it faster to set up compared to more centralised alternatives, potentially also allowing for low bureaucracy for funding recipients, as well as flexibility in how funding is disbursed and reported. Another key advantage lies in the possibility to ensure EU-level branding and strategic visibility, avoiding the mission dilution or fragmentation that can occur in the embedded model.

Despite its significant advantages compared to other governance options, though, substantial challenges remain for implementing this model. The hybrid nature requires strong coordination and trust across Member States, and potentially risks the dominant influence of some Member States to the exclusion of other, perhaps under-represented, voices. A weak central node may risk fragmentation;

conversely, excessive centralisation may lead to bottlenecks or perceived overreach. A clearly defined mandate, cross-cutting and meaningful involvement of industry, Member States and other relevant stakeholders, a well-defined strategic focus, and the adoption of streamlined, fit-for purpose operational mechanisms would be essential for success.

5.1.4. Decentralised framework under common policy guidelines

This model delegates funding, administration, and implementation responsibilities for certain policies entirely to individual Member States or independent organisations, while unified under a broad EU strategic framework. In short, the EU establishes the strategic approach or sets minimum standards under the 'common policy guidelines,' while implementation is decentralised. Those guidelines create a non-binding and typically broad framework for future acts in a specific policy area. Therefore, the EC's role is largely limited to evaluating performance and encouraging compliance through soft governance tools such as reporting, benchmarking, and voluntary coordination mechanisms – unless those 'future acts' take the form of legally binding instruments, which Member States are obligated to implement and for which the EU may pursue formal enforcement measures such as infringement procedures.[190]

Overall, this model embraces a 'free-for-all' approach to policy implementation rather than joint execution. This is comparable to how some EDICs or IPCEIs operate but typically with more limited centralised control. One example is the EU's relatively loose coordination of employment and social policy (European Pillar of Social Rights).[191] This approach generally allows maximal flexibility through enabling diversity and localisation of implementation efforts to the domestic context. It also encourages political and administrative buy-in from Member States, while maintaining unity on EU strategic frameworks.

However, this kind of decentralised approach may risk undue complexity, inefficiency including through duplication and systematic fragmentation – since the quality and pace of implementation may vary widely across Member States. Within the digital sphere, that implementation may vary not only depending on administrative capabilities, political will and unequal funding capacities, but also the status of digital development. Smaller or less digitally mature Member States may struggle to match contributions or launch comparable initiatives. That challenge was evident in the efforts to create a Digital Single Market (DSM), which seeks to create a unified digital marketplace across the EU. While many Member States have gained ground in their digital transformation, low levels of digital skills and investment may hamper future growth and deepen the digital divide.[192]

This model would also require a significant amount of supporting institutional infrastructure. That includes the support of corresponding legislation or a regulatory framework, strong coordination mechanisms, and commitment at both the EU and national levels to ensure equitable and effective results across the region, all of which could be difficult to implement. Without an overarching and coordinating structure, shared goals around security, innovation, autonomy, resilience, and competitiveness could become diluted, and duplication of efforts or gaps in support may persist. That is a less appropriate solution given the importance of pooled resources and coordination for the EU-STF's objectives and structure.

5.2. Detailed Analysis of Institutional Setups

Of the governance options considered for the EU-STF, the standalone and centralised fund, and the hybrid/shared management structure or coordination model emerge as the two most compelling categories for deeper analysis. That said, they have different strengths, much of which relate to the core question of their potential feasibility. To consider this feasibility, we will evaluate the seven criteria identified in Section 4.4.3, specifically: pooled financing and coordination, low bureaucracy, political independence, flexible funding, community focus, strategic alignment, and transparency.

While both options are analysed in accordance with these criteria, we conduct a more systematic review for the hybrid/shared management structure or coordination model than the standalone and centralised model. This is because the latter would require new legislation for its establishment, making any assessment conditional on that outcome and giving the EU some flexibility in designing it to meet many relevant criteria. That includes flexibility in funding disbursement or mechanisms for working with the ecosystem on funding prioritisation. By contrast, when considering hybrid models such as EDICs or JUs, the extent to which they meet the criteria can be assessed more definitively, as their governance and operational structures are already more well-defined (although EDICs have considerable flexibility subject to their setup and – a strength we will highlight later).

5.2.1. Summary of argument

The standalone and centralised fund offers a bold and coherent institutional vision: a centralised entity with a distinct budget line, legal mandate, and political visibility, meeting the level of ambition presented in Sections III and IV. It sends a strong signal of EU-level commitment to digital sovereignty, cybersecurity, and competitiveness, while helping to ensure mission integrity and strategic clarity. Despite significant complexity in its setup and risks of administrative inertia, the model's potential for concentrated oversight and high-level impact aligns well with the EU-STF's ambition to address systemic under-investment in open digital infrastructure. Moreover, a centralised model could more easily harmonise with strategic digital policy goals at the European level, even if its implementation would require extremely careful consideration of transparency, agility, and political independence, as well as a strong coordination with existing funding mechanisms and the open source community.

At the same time, the hybrid/shared management structure offers an expedient, highly pragmatic, and politically viable alternative, balancing EU-level direction with flexible implementation and co-investment, in line with the expressed interests of many stakeholders during the interviews for this study. Instruments like JUs, EDICs, and IPCEIs allow for shared governance between the EU and Member States, pooling resources and enabling distributed participation from public and private actors alike. This structure offers the potential for more agile implementation, reduced administrative overhead, and more community-aligned investment while maintaining strategic coherence. Crucially, it could help bridge the gap between Brussels and regional innovation ecosystems, addressing critiques of over-centralisation while ensuring visibility and coordination through a well-defined central node.

As such, both the standalone and centralised fund and the hybrid/shared management structure or coordination model offer different but complementary routes for meeting the EU-STF's goals. The former favours institutional strength and strategic unity, the latter responsiveness, legitimacy, and

distributed resilience. We will argue that the latter offers the most realistic and short-term model for the EU-STF's proposed objectives and structure, in line with the history/character of the German STF and the expert insights of those interviewed in setting up an EU-STF. Below we will present an analysis for both options.

5.2.2. 'The Moonshot Model': Analysis of standalone and centralised fund

A standalone and centralised fund represents the most institutionally ambitious approach to establishing EU-STF. This model seeks to create a dedicated budget line and governance structure. Under this model, the EC, most likely (though not definitely) through DG-CNECT, would directly manage the EU-STF. In doing so, it could entrust the executive tasks either to an existing agency such as HaDEA or to a newly created agency. This approach would need to be established under the auspices of new or proposed legislation, or through the amendment of existing legislation, with budget allocated via the upcoming MFF negotiations.

That said, although this setup has these advantages, it also entails specific trade-offs in areas such as agility and community engagement. Centralisation carries many risks, including bureaucratic inertia, political vulnerability, and reduced responsiveness to the needs of a distributed open source ecosystem. Without intentionally addressing these considerations from the outset, the fund risks becoming a failure before it is even implemented or off the ground.

The legislation that creates or empowers such a fund must enable the governance and disbursal of its funds to be simpler than previous EU funds. Funding applications which are more like the Horizon Europe programme's and less like the NGI's cascade funding model would risk alienating open source developers and community members and introduce high levels of bureaucracy and administration into an area which demands simpler funding disbursal and reporting procedures. This would not align with the needs of open source developers, who often do not have a professionalised supporting workforce to support the acquisition and use of new funding. Moreover, unlike some existing programmes, recipients of funding must not be limited to legal entities based in the EU, due to the global and distributed nature of the open source community. Funding would have to reach different entities, including individuals, companies who employ developers to work on OSS, etc – not just in the EU but in other parts of the world as well.

Moreover, the fund must enable a reasonable amount of political independence. The mandate of the German STF has been enabled by political independence. In the EU context, there is a lot of bureaucracy, which makes many funding programmes subject to more scrutiny. Given the cross-cutting and foundational nature of open source developer support, a governance setup which enables continued re-review of the fund's activities or structures – or makes it a political football – would be a negative outcome. A centralised fund should create mechanisms for input from the open source community, allowing them to inform funding decisions and processes which can be introduced rapidly. It should also have a strong degree of coordination with the activities of Member States and industry.

Funding delegated to an existing executive agency (e.g. HaDEA)

The Regulation setting up the EU-STF could expressly allow for the delegation of consistent

operational responsibilities to an executive agency, in order to ensure sound financial management and an efficient budget execution. This is in line with Art. 69 of Regulation (EU) 2018/1046, which explicitly allows the EC to delegate the implementation of EU programmes to executive agencies to ensure an efficient financial management, and consistently with established practices. This governance approach is formalised through an EC Commission Implementing Decision, which clearly sets up the executive agency's responsibilities. These include organising open funding calls or calls for proposals, coordinating the evaluation processes, concluding grant agreements, and ensuring the reporting and monitoring of funded activities. This way, the EC would retain full control over the key objectives of the EU-STF while relying on the agency's capacities to handle day-to-day operations efficiently.

Since HaDEA already manages programmes of a similar scope, it might be both pragmatic and efficient to entrust it with the operational dimensions of the EU-STF, at least in the short-term. HaDEA plays a crucial role in operationalising funding for health, digital, and infrastructure-related initiatives. While it might not be an ideal fit to host or manage the EU-STF — at least not in its core conception as a strategic, community-anchored investment instrument for open digital infrastructure – it is one of the few examples of a structure which might support the operationalisation of a transitional or limited version of the EU-STF. In particular, its experience in administering complex multi-sectoral programmes could prove valuable in piloting early-stage funding streams, while more permanent and mission-driven solutions are developed. A useful parallel can be drawn with Germany, where the STF was first incubated within SPRIN-D, the aforementioned Federal Agency for Disruptive Innovation in Germany,[193] before spinning out into its own dedicated legal structure as the Sovereign Tech Agency — a phased approach that could similarly be considered at EU level.

HaDEA has some distinct advantages over other EU agencies and funds. Several executive agencies are already in place, such as the European Innovation Council and SMEs Executive Agency (EISMEA)[194] – which focuses on SME commercialization and innovation under the EIC – or the European Climate, Infrastructure and Environment Executive Agency (CINEA)[195] – which oversees programmes in areas such as energy, climate, and transport. But while these agencies could in theory be adapted for such tasks, in practice they are less naturally suited to the digital and open source infrastructure objectives of the EU-STF. By contrast, HaDEA is already responsibile for digital sovereignty-driven calls under CEF Digital or DIGITAL. For example, HaDEA is currently managing the EUR €20 million CEF Digital call for 'Operational Digital Platforms',[196] which aims at funding secure, cross-border digital infrastructures in the energy and transport sectors.

Establishing the EU-STF under the EC's centralised management, with the executive part allocated to HaDEA, is not without trade-offs. Its broad scope, covering programmes not only in the digital sphere, but also in health through initiatives such as EU4Health, suggests that it is not an entirely natural fit for the EU-STF. Culturally, it might be tough to introduce the type of funding and governance the EU-STF demands into an existing institution, one with its own procedures that might be harder to adapt than in a new body, or in a decentralised model. Furthermore, leaving the implementation of the EU-STF to HaDEA could overburden an agency already tasked with managing multiple programmes, potentially leading to negative impacts on delivery.

For these reasons, HaDEA may only be considered as the executive agency for the EU-STF in the short-term. In the long-term, a new agency, potentially called EDIEA, could be set up. Such a novel

agency, if designed well, could emulate characteristics of the German STF and serve as an ecosystem strengthener and trusted actor for the open source community.

Criteria Analysis

1. Pooled Financing: While pooled funding from multiple actors could, in theory, expand the financial base on the EU-STF and encourage a broader engagement of the stakeholders, it would raise immediate coordination challenges that risk diluting the strategic focus of the fund. In the short-term, exclusive funding through the EU budget offers a more stable foundation, thus avoiding the fragmentation and the governance concerns that multi-source financing would inevitably entail.

2. Low Bureaucracy: Even though there may still be administrative burdens due to specific calls and requirements, it is possible to design the funding in order to reduce the administrative load. Some funding mechanisms such as Horizon Europe often rely on lump sums[197] or small grants, which reduce paperwork and financial reporting. There is also the cascade funding model, which may require some tweaks to make it even more straightforward and work in the case of HaDEA.

3. Political Independence: HaDEA is headed by a Steering Committee composed of Directorate-General for Health and Food Safety (DG-SANTE) staff and Directorate-General for Research and Innovation (DG-RTD), for DG-CNECT, for DG-GROW and for Defence Industry and Space (DEFIS).[198] This structure, which involves several DGs, ensures a model of distributed governance, drawing on the expertise and strategic priorities of multiple policy areas. At the same time, HaDEA enjoys administrative independence, allowing it to implement EU programmes efficiently and with technical autonomy.

4. Flexible Funding: There are flexible fund disbursement options which could possibly be considered, though this would need to be carefully considered against the mandate of HaDEA. For instance, rolling calls or a version of cascade funding (such as the NGI's precedent), might be possible, but would also likely be challenging given the way other funds are distributed by HaDEA.

5. Community Focus: HaDEA does not set funding priorities, as these come from the EU's political decisions and work programmes. However, for instance, information days are an available option in use.[199] It is possible that the agency could delegate more input for the administration of open source funding in particular.

6. Strategic Alignment: Although not specifically targeting open source, HaDEA already manages calls from CEF Digital and DIGITAL, aligning with priorities in skills, digital transformation, infrastructure, and public services. By sitting within the control of DG-CNECT, it also broadly aligns with other EU digital policy ambitions.

7. Transparency: HaDEA applies clear transparency rules in line with EC Decision (ECD) 2024/3082.[200] These include that anyone who wants to meet HaDEA managers must be registered in the Transparency Register. Furthermore, the details and meeting summaries are published within two weeks. This guarantees openness about who meets with HaDEA.

Strengths

- HaDEA has extensive experience with major funding mechanisms such as DIGITAL and CEF Digital, thus ensuring expert management of projects in the digital domain.
- HaDEA's mature operational processes allow it to capitalise on existing systems and expertise, ensuring the smooth implementation of the EU-STF.

Weaknesses

- Leaving most of the EU-STF executive management to HaDEA may strain its already broad workload, risking oversights, gaps or slower evaluations.
- HaDEA's mandate centers programmes in the health and digital sphere, lacking tailored expertise in open source governance or community-driven funding.
- HaDEA does not seem like a long-term cultural or institutional fit for fulfilling the proposed mandate of the EU-STF, which is drawn from the pioneering work of the German STF.

Fund directly managed as a new, independent executive agency

While HaDEA offers an adequate interim solution, in the longer term, a new executive agency called EDIEA could be established. In line with Art. 3 of Council Regulation (EC) No 58/2003[201] on the setting-up and winding-up of executive agencies, the EC may (following a cost-benefit analysis) decide to establish an executive agency for the purpose of entrusting it with specific tasks relating to the management of the EU-STF.[202] The EC shall also determine the lifetime of such an agency, which will possess legal personality.[203]

The establishment of such a body, through a ECD, would provide a dedicated operational framework targeted to achieve the objectives of the EU-STF. It would also ensure procedures that are sufficiently flexible and adapt to the needs of SMEs and small open source communities, which are often constrained by the administrative burdens of existing funding mechanisms already in place. Furthermore, a dedicated body is essential to address the specific needs of the open source ecosystem, which are not currently targeted by the EU's existing executive agencies.

However, the setting up of a potential EDIEA is not without challenges. It requires a clearly articulated timeline, accompanied by a multi-stage approach that allows for a gradual capacity-building. This architecture must be supported by a robust governance, including a steering committee for strategic oversight, a director responsible for daily operations, and an adequate staff to ensure efficiency, transparency and accountability throughout the agency's lifetime.[204] The EU Court of Justice's case law on the creation of executive agencies would need to be accounted for when experimenting with novel governance arrangements.[205]

In addition, the novel institution should closely coordinate with bodies that have similar scopes, such as HaDEA itself, in order to avoid duplications and maximise its impact. For these reasons, the establishment of this agency remains a long-term objective, while in the short-term the executive functions should be carried out by HaDEA or directly by the EC via DG-CNECT.

Criteria Analysis

1. Pooled Financing: While the creation of a dedicated executive agency could, in the long-term, enable pooled financing tailored specifically to the needs of open source maintenance, this would require significant upfront design and coordination efforts. In the short-term, reliance on HaDEA or DG-CNECT would limit the scope for innovative pooled mechanisms until the EDIEA builds the necessary governance and operational capacity.

2. Low Bureaucracy: There would be significant financial, administrative, and operational burdens in setting up a new agency (due to the necessity to set up governance systems and procedures). There is a risk of creating cumulative institutional bureaucracy or inertia, which risks diluting the impact of the EU-STF. To be effective, the new institution should be closely aligned with the open source community it serves, with streamlined procedures as a key priority.

3. Political Independence: While some level of political independence could be guaranteed, it would be tricky for the fund to maintain this in practice, particularly if the fund were based in Brussels. For this reason, political independence would need to be a key focus during the design phase.

4. Flexible Funding: Such a standalone and centralised fund under EDIEA could allow for flexibility and calls can be targeted to the need of smaller actors. This could, for example, build on the cascade funding model. However, this would require significant maneuvering from the outset to make this a different vehicle than what has come before.

5. Community Focus: This is in theory entirely viable. That said, if the design of the fund proves complicated, it could risk distancing the open source community and dis-incentivising them from supporting the fund, should it go in a direction they deem unfit for purpose.

6. Strategic Alignment: This approach would offer strong institutional branding and visibility. It would enable close alignment with EC priorities, so the main consideration would be to make sure that does not dilute the impact or focus of the fund on open source maintenance specifically.

7. Transparency: Setting up a new executive agency offers the possibility to set up transparent procedures, without the need to adhere to existing frameworks.. Therefore, transparent procedures, designed from scratch, can be created in order to reflect the fund's specific values.

Strengths

- Possibility to establish flexible and transparent procedures which could be ideal also for smaller actors.
- The executive management of the EU-STF would be specifically targeted to its needs.

Weaknesses

- Possible overlaps with the mandate of HaDEA or other existing agencies .
- Difficult to set up, and the process can also be quite lengthy.

5.2.3. 'The Pragmatic Model': Analysis of hybrid/shared management structure or coordination model

Given the political expediency (but also limitations and complications) of setting up a standalone and centralised fund, a hybrid/shared management structure or coordination model appears politically and operationally viable, particularly in the short-term. This is not to say that some elements of what the hybrid model does could not be supported by centralised function. Rather, the success of this approach hinges on the legal instrument selected for coordination and implementation. And it requires a significant engagement with the open source community to preserve the distributed and collaborative nature of OSS development, as well as to build the institutional muscle necessary to set up fund disbursement vehicles that are better aligned with the character and needs of the community as a whole..

Three possible vehicles are especially relevant for unlocking and capitalising the scale of investment necessary for an EU-STF under this approach. These include: JUs, EDICs, and IPCEIs. Those funds do not serve as a stand-in for the EU-STF on their own, and require a strong coordination with the German STF and potential future bodies that might be built up either within or between Member States. Below we overview the three setups and then analyse the suitability of JUs, EDICs, and IPECEIs based on seven key criteria, which were developed based on the interviews conducted for this study. Indeed, the criteria are based on extensive stakeholder engagement via the interviews and workshops conducted for this project. They are: pooled financing, low bureaucracy, political independence, flexible funding, community focus, strategic alignment, and transparency.

Overview

Joint Undertakings

JUs, set up under Article 187 of the Treaty on the Functioning of the European Union (TFEU),[206] offer strong capacity for pooling EU, Member State, and private sector resources. Their establishment requires a Council Regulation under Article 188(1) TFEU,[207] following an EC proposal and consultations with the European Parliament and European Economic and Social Committee. In practice, most of the JUs have been set-up under Regulation (EU) 2021/2085 ('Single Basic Act')[208] which currently regulates nine key JUs under the Horizon Europe Research and Innovation Framework Programme. Seven JUs that were already active under the Horizon 2020 programme,[209] have continued into the Horizon Europe framework as newly established legal entities, operating under updated names and expanded or revised mandates. Two JUs are newly created.[210]

JUs have their own legal personality and administrative autonomy, making them capable of managing large multi-actor research and innovation (R&I) investments over long timeframes. Existing JUs (e.g., EuroHPC JU, SESAR JU) demonstrate how they can centralise high-tech strategic investments and deliver complex information ecosystems. They also crucially allow for the involvement of private sector funds on top of contributions from the EU and Member States, potentially unlocking an investment scale necessary for the EU-STF's success.

One recent example offers insight into the scale of potential financing for an EU-STF-like effort via a JU. The Chips JU[211] is a publicly funded, EU–Member State–industry partnership founded in 2023 under the European Chips Act and the broader 'Chips for Europe' initiative.[212] Its mission is to fortify Europe's semiconductor ecosystem by financing cutting-edge pre-commercial pilot lines, deploying a cloud-based chip design platform, and fostering a network of competence centres to support SMEs, start-ups, universities, and larger companies.[213] With an expected budget of approximately EUR €11 billion by 2030 (including nearly EUR €1.67 billion from the EU and matching national contributions), Chips JU aims to bridge the gap between research, innovation, and industrial-scale manufacturing.

Although JUs are typically more innovation-driven, focusing on the development of cutting-edge technologies, several JUs are also playing a role in long-term infrastructure maintenance. For example, since its creation in 2018[214] and subsequent update,[215] the EuroHPC JU has deployed, maintained, and continuously upgraded one of the world's leading high-performance computing infrastructures, with supercomputers such as Large Unified Modern Infrastructure (LUMI),[216] Leonardo and MareNostrum. Moreover, EuroHPC has launched initiatives in training, competence centres, and support-services that ensure the long-term sustainability and impact of these capabilities.[217]

Through enabling industrial contributions, the Chips JU and the EuroHPC JU showcase the potential of JUs; although the development and setting up of this model is not without challenges. Due to their multi-actor nature, JUs are complex vehicles, requiring a high degree of coordination and delicate stakeholder management. Moreover, they are perhaps more ideally suited for projects with stronger and well-defined industry supply chains, particularly ones with tangible real-world artefacts that are easy to persuade policymakers of. They are also generally less suited for long-term maintenance, and more suitable for innovation-driven projects.

Strengths

- High capacity for integrating funding streams across EU, Member States and industry.
- High degree of flexibility in allowing both financial and in-kind support.
- Suitable for long-term and large-scale strategic investments, as JUs are established under EU law for a relatively extended timeframe.
- Well-established centralised governance mechanism, with industrial involvement possible.

Weaknesses

- More innovation-driven, possibly less suitable for maintenance-oriented goals.
- Legally and politically complex to establish and to adapt over time; requires a full legislative act (Council regulation).
- Risk of centralisation and bureaucratisation may discourage more informal and grassroots OSS projects.

European Digital Infrastructure Consortia

Created under the DDPP Decision, EDICs are a significant new implementation mechanism for Member States to collectively develop and operate digital infrastructures. They were inspired by European Research Infrastructure Consortia (ERICs), but differ in terms of primary focus, namely favouring 'deployment and industry, not research as was the case for ERICs'.[218] Their main objective is to provide a legal framework to invest in MCPs that Member States cannot set up individually, given their

scale, while enabling speedy establishment, flexible implementation and facilitating coordination of funding to incentivise Member States.[219]

Each EDIC has a distinct legal personality. These legal personalities are consistent with the principle of institutional autonomy and the objective of limiting liability to that entity rather than imposing risk upon individual Members (beyond their committed contributions) and the EU. To establish an EDIC, at least three Member States must apply and receive approval from the EC. The statutory seat of an EDIC must be based in a participating Member State and all Member States must recognise its legal personality. The founding Member States define its statutes, which determine governance structure and other functioning rules. Membership may be open to entities other than a Member State (e.g. third States, international organisations of European interest, public and private entities) as stipulated in those statutes. However, Member States must hold the majority of voting rights, regardless of the amount of contributions from other entities. And membership must remain open for all Member States on fair and reasonable terms.

The EU has so far established three EDICs to drive cross-border digital collaboration and coordination on funding, while ensuring common standards and interoperability. Alliance for Language Technologies EDIC (ALT-EDIC)[220] focuses on building a multilingual AI and language technology infrastructure, European Blockchain Partnership and European Blockchain Service Infrastructure EDIC (EUROPEUM-EDIC)[221] governs and expands the European Blockchain Services Infrastructure, and the Networked Local Digital Twins towards the CitiVERSE EDIC (LDT CitiVERSE EDIC)[222] connects local digital twins into a shared urban planning and simulation platform. At the date of publication, several other EDICs, such as a Digital Commons EDIC and a Cybersecurity Skills Coalition EDIC (CSC-EDIC), are in the planning stages or awaiting approval and entry into effect.[223]

These EDICs advance digital infrastructure initiatives like Europe's digital sovereignty in AI, blockchain, and smart cities. A fund that pools financing and allows for coordination around open digital infrastructure seems like a natural extension of these efforts. A key advantage is a distinct flavour of an EDIC, e.g. a legal personality and flexible governance setup depending on the structures and objectives of the consortium as defined in its statutes. EDICs may allow for flexible membership (Member States, private entities, etc) and funding structures and sources. For the budget, Member States may provide funding, in-kind contributions (such as data, infrastructure, or expertise), or a combination (provided that there is sufficient funding to establish it). However, it may supplement its budget with other sources of revenue, which may include private sources and relevant EU and national grants, such as from DIGITAL, Horizon Europe and CEF Digital.[224]

Subject to its statutes, the level and type of contribution may influence voting rights. For instance, the ALT-EDIC statutes has indexed the voting rights of its Members to the value of contributions with a maximum three votes available for Members making annual contributions from EUR €500,000.[225] Only Member States or regions in the European Economic Area (EEA) are eligible for membership in that entity, but that does not preclude donations from alternative sources. Meanwhile, the votes of Members of EUROPEUM-EDIC are not tied to the value of their contributions. But they must make a minimum financial (EUR €150,000) and in-kind contribution.[226] Other entities, such as international organisations with a European dimension, may become Members or Observers, yet their votes weigh comparatively less than those of Member States, who hold ultimate decision-making power.

While still pending EC approval, the Digital Commons EDIC could offer a precedent for a coordinated open source governance financing and coordination. On 8 July 2025, France, Germany, Italy and The Netherlands signed the EDIC application and submitted it for EC approval.[227] That EDIC reportedly aims to support the development, maintenance and scaling of digital commons, such as OSS, open data, open content, and open standards.[228] Its objectives include creating a central hub for technical, legal, and funding assistance to empower European digital commons projects, while ensuring they align with values like transparency, equality, and digital sovereignty. While details are forthcoming, the EDIC would mark a welcome investment in the digital commons.

The EU-STF would be a natural partner for the Digital Commons EDIC in the pursuit of certain aligned yet distinctive objectives and via different yet complementary tools. For instance, the EU-STF would be a dedicated expert mechanism for supporting pooled financing and contribution of funding for long-term maintenance of OSS, while the latter shall reportedly assume a 'facilitator' role in helping stakeholders to navigate the funding landscape.[229] Moreover, the EU-STF has a focus on advancing OSS cybersecurity and ODBTs, while the Digital Commons EDIC seems more oriented towards end-user applications and services precisely because of its focus on 'digital commons'.

Likewise, the pending CSC-EDIC offers another potential example, both in engaging diverse stakeholders and in coordinating with EU legislation, initiatives and organisations in pursuit of improved cybersecurity. Greece has led the development of that application as part of a consortium including Cyprus, Austria, Croatia and Slovenia. If successful, it is expected to become operational by the end of 2025.[230] Relevantly, the CSC-EDIC aims to strengthen the cybersecurity competencies of relevant EU organisations(e.g. EC, ENISA and European Cybersecurity Competence Centre), through effective implementation of the Cybersecurity Skills Academy initiative; upskill targeted professionals, especially SMEs and public administrations; and consider alignment with requirements of recent EU legislation and initiatives, encompassing the NIS2 Directive and CRA.

Strengths

- Close strategic alignment, as it is designed specifically for digital infrastructure collaboration.
- Legal identity limits liability for Members and the EU, while flexible and dynamic governance structures are possible under the statutes, including coordination with industry and the OSS community.
- Permits the pooling of contributions from diverse actors and sources (e.g. financial and in-kind contributions).
- Flexible and responsive to national and other contexts.

Weaknesses

- A nascent mechanism that is still relatively legally and operationally untested.
- Generally driven and run by a subset of EU Member States, potentially hindering EU-wide relevance and developing statutes that align with their interests, although they must remain open to the participation of all Member States on fair and reasonable terms.
- Initial onus for funding lies upon Member States, although private and EU sources may supplement that once the budgetary requirements are satisfied.
- Possibly less attractive governance models for private and other non-Member State actors since they receive comparatively less voting rights even if they invest. However, there is a spectrum of options available, whereby they may be Members who can still vote,

- Observers, or only have the ability to observe or donate.
- Some precedents for the EDIC point to a volume of financing much less than the scale/ambition the EU-STF might otherwise call for. For example, in the case of the Digital Commons EDIC, it will (once approved) have only around EUR €5.3 million in initial budget, with the EU funding almost EUR €2.5 million of the EDIC budget and Member States contributing over EUR €2.8 million to start.
- Flexible yet highly variable structures and principles based on the founding Member States and the statutes they adopt. That may mean, amongst other factors, less control or coherence if not backed by strong EC leadership or central secretariat.[233]

Important Projects of Common European Interest

Under Art. 107(3)(b) TFEU,[234] IPCEIs allow Member States to provide state aid to strategic projects that benefit the EU overall. To be eligible for support, a project must align with strategic priorities set by the EU and involve the active participation of multiple Member States. It must also secure substantial private investment from the participating companies. Importantly, the project should deliver wide-reaching benefits that extend beyond the direct participants, helping to minimise any negative effects on competition within the internal market. Additionally, it should demonstrate a high degree of ambition, particularly through advanced research, development, and innovation efforts.[235] IPCEIs are designed for state aid recipients.[236] Accordingly, this model would only suit OSS maintenance if maintainers of critical open source projects can receive subsidies either directly or via corporate structures.

To set up an IPCEI, generally at least four Member States must jointly define their strategic scope and objectives,[237] ideally facilitated by the Joint European Forum for IPCEI (JEF-IPCEI) platform.[238] Subsequently, they need to run national calls to select projects that meet these goals and IPCEI criteria, ensuring that all projects collectively form a coherent, cross-border initiative. Finally, Member States notify the EC, which assesses projects under the IPCEI framework.[239] Since 2018, several IPCEIs have been approved by the EC, including two IPCEIs on Microelectronics (2018, 2023)[240] and an IPCEI on Next Generation Cloud Infrastructure and Services (2023). Although not institutions per se, they function as project-based coordination frameworks and can mobilise substantial national co-funding under shared governance arrangements.

The second IPCEI on Microelectronics and Communication Technologies (IPCEI-ME/CT)[241] is a notable example of how the framework can facilitate coordinated state aid for strategic cross-border projects that advance shared European priorities. The project brings together 14 Member States to support a large portfolio of R&D and industrial projects. It also includes 68 projects led by 56 companies, complemented by over 30 associated participants. Participating Member States have committed over EUR €8.1 billion in public funding, intended to draw in approximately EUR €13.7 billion in private investment. Its mission is to support the EU's digital and green transitions by developing advanced microelectronics solutions and resource-efficient manufacturing processes, with expected impacts for 5G/6G, autonomous driving, AI, quantum computing, and energy systems.[242]

This example shows how the IPCEI model enables significant mobilisation of public and private resources for high-risk, large-scale industrial innovation. That said, its design may be less well-adapted for fostering more open, decentralised innovation ecosystems, such as OSS development and maintenance models or open innovation with broader collaborative R&D communities.

Strengths

-Flexibility in coordinating national investments.
-Effective for unlocking national budgets beyond state aid rules.
-No new institutional setup required; relatively rapid deployment possible.
-No formal maximum aid threshold.

Weaknesses

-Fragmented project governance; no standing entity for ecosystem support.
-Requires complex national coordination, EC approval and a complicated application procedure.
-Better suited for R&D and first industrial deployment within vertically integrated industrial investments than OSS maintenance.
-Uneven capacities both across Member States and among companies may limit participation in IPCEIs, distort competition and widen economic and technological gaps.

Criteria #1: Pooled Financing

Joint Undertakings

JUs combine EU funding with contributions from other participating stakeholders, including Member States and private entities. In terms of EU budget, JUs are primarily funded by Horizon Europe, but they may also receive funding from other EU programmes, including CEF Digital and DIGITAL. These financial contributions are supplemented by contributions by other actors, which may be both financial and in-kind. For instance, the EuroHPC JU under the current MFF receives a total contribution of EUR €3 billion from the EU budget, including EUR €1.9 billion from the DIGITAL, EUR €900 million from Horizon Europe, and EUR €200 million from CEF. Participating States match that investment, while private members contribute with EUR €900 million, both financially and through in-kind contributions.[243]

European Digital Infrastructure Consortia

Enabled by their flexible, agile and tailor-made governance structure – and subject to their statutes – EDICs are a viable mechanism for pooling funding and contributions from diverse sources (Member States, EU projects, private sector, etc) and of different types (including financial and in-kind contributions). The latter may encompass useful platforms or services to the EU-STF, such as expert advice or the delivery of security training to OSS developers. While a wide range of relevant actors may contribute funding or other forms of support, much depends on the statutes – including whether they have a defined governance role and are eligible to become Members and enjoy voting rights. Existing and proposed EDICs have emphasised the importance for effectively realising their mandate of drawing on diverse funding sources and other contributions, rather than limiting themselves to EU and Member States' budgets.

Important Projects of Common European Interest

IPCEIs are primarily designed to allow EU member states to support strategic cross-border projects that are crucial for EU's competitiveness and resilience. Therefore, the primary source of funding comes from member states, even though many IPCEIs strongly rely on private investments. For instance, considering the IPCEI Next Generation Cloud Infrastructure and Services (approved on December 5,

2023), seven member states - including France, Germany, Hungary, the Netherlands, Italy, Spain and Poland - are expected to pool approximately EUR €1,2 billion, while private actors are expected to contribute EUR €1,4 billion.[244]

Criteria #2: Low Bureaucracy

Joint Undertakings

JUs are governed under EU public law with formal, often complex, administrative and reporting requirements. For instance, generally JUs follow financial rules aligned with Horizon Europe, including ex-post audits by the EC's Common Audit Service (CAU).[245] They also require a considerable mix of officials, staff and national experts to perform their functions, adding to the overall administrative burden.[246] While JUs' obligations are designed to ensure sound financial management and high levels of accountability, they can impose a significant compliance burden, especially on smaller actors that often lack capacity to meet these demands.

European Digital Infrastructure Consortia

In theory, EDICs offer more flexibility because the statutes and implementing rules and procedures can prioritise simplified reporting and administrative processes, as agreed by founding Member States or where amendable. In the best case scenario, this can enable lighter-touch, more proportionate oversight, particularly where in-kind contributions and diverse stakeholder participation are significant. If designed with this in mind, EDICs could allow for adoption of cascade funding from a variety of sources, milestone-based reporting, or adaptive approaches that reduce burdens while maintaining transparency and accountability. That said, this depends a lot on the design of the statutes and related governance structures, which could accumulate complexity as the entity evolves and/or as more stakeholders are involved. There is also a chance that founding Member States – perhaps, especially the host State – have established practices in terms of project administration and reporting that they want to duplicate in the EDIC, for better or worse.

Important Projects of Common European Interest

IPCEIs are Member-state led, meaning that Member States define the project's objectives, select the participating companies – ideally, through transparent and competitive processes – and establish appropriate governance arrangements for the project. Since the financial contributions provided by Member States qualify as State aid under EU law, they must be formally submitted to the EC for review. Before granting approval, the EC evaluates whether the proposed projects comply with the IPCEI framework and State aid rules.

In practice, the administrative burden depends greatly on the Member States involved and how they engage through the IPCEI. Some actors may offer streamlined processes, while others may impose detailed national reporting and compliance rules; it can be difficult to standardise. Larger Member States, equipped with more robust administrative structures and greater experience in engaging with the EC, are often better positioned to effectively support the enterprises they wish to promote[247]. This inconsistency can complicate participation for actors operating across borders and efforts to establish predictable, low-burden requirements.

Considerations on IPCEIs' administrative burdens are also explicitly reflected in the Directorate-

General for Competition (DG-COMP) Code of Good Practices. This document explicitly states that 'before designing an IPCEI, national authorities should consider that the manageability of an IPCEI is also an essential factor. IPCEIs with a large number of individual projects unavoidably take longer to coordinate, design, and assess'.[248]

Criteria #3: Political Independence

Joint Undertakings

JUs are typically headquartered in Brussels and function as centralised entities governed jointly by public and private actors. While the exact composition may vary across initiatives, each JU is generally structured around some core bodies: a Governing Board, an executive Director, a States' Representative Group (except when States are already represented in the governing board), and in many cases a Scientific Advisory Body. The Governing Board – including representatives from the EC, industry and research organizations – provides strategic direction, and oversees coordinated implementation.[249]

Many JUs[250] operate under a bipartite model, with the EC and private industry/ research members sharing governance and contributions. Some JUs – such as EuroHPC – use a tripartite model, adding either participating States or an intergovernmental body to the Governing Board.[251] While this governance model offers strategic coherence, it may also pose challenges for inclusive participation, potentially limiting the engagement of grassroots actors and weakening local ownership. Indeed, although JUs often include advisory bodies that engage multiple stakeholders, their predominantly centralised structure and their operations, which are mostly based in Brussels, may hinder participation of Member States or other smaller actors.

Finally, JUs have their own legal personality and the broadest legal powers allowed under national law in all EU member states. They can operate independently and be held accountable. In fact, JUs can have their own property, sign contracts, and take part in legal proceedings.[252]

European Digital Infrastructure Consortia

EDICs enable flexibility in choosing a distributed governance option, subject to the Statutes and other governance documents. For instance, Member States may elect to host nodes or national secretariats, and EDICs can contract out functions, create networks that drive industry partnerships and provide solutions for common challenges,[253] or build regional hubs, making them ideal for a federated model. This could mirror the design of academic research infrastructures, like ERICs, which inspired the EDIC model although they have different key purposes. Experts and other stakeholders may participate in various manners and through different mechanisms to support those governance structures and processes, such as through technical or expert advisory boards.

Finally, the EDIC's distinctive legal status arguably lends itself to independence and accountability while limiting liability to the EDIC itself, rather than Members (beyond their pledged contributions) and the EC. In approving all three standing EDICs (ALT-EDIC, LDT CitiVERSE and EUROPEUM-EDIC), the EC has emphasised that they:

> *shall have legal personality, and it shall enjoy, in each of the Member States, the most extensive legal capacity accorded to legal entities under the law of that Member State. It may, in particular, acquire, own and dispose of movable, immovable and intellectual property, conclude contracts and be a party to legal proceedings.*[254]

Important Projects of Common European Interest

IPCEIs function through decentralised funding of nationally hosted projects. Nevertheless, mechanisms, such as the Design Support Hub,[255] may offer technical assistance for Member States in streamlining the project's design and preparing them for assessment. Furthermore, the JEF-IPCEI[256] aims at identifying priorities and improving IPCEI's effectiveness, providing platforms for coordination and exchange of best practices between the EC, Member States, and potentially other stakeholders. However, these mechanisms often fall short of establishing a shared governance framework or a clear institutional identity, making it more challenging to develop a long-term strategy.

Criteria #4: Flexible Funding

Joint Undertakings

JUs typically require high levels of reporting and administrative oversight, aligning more with Horizon Europe-style frameworks. Their funding mechanisms generally follow the Horizon Europe grant agreement structure, including competitive calls for proposals and formal grant agreements. Calls for proposals also specify the objectives, eligibility criteria and awarding conditions. This could make JUs less suited for most OSS maintenance and smaller community projects, which require low-burden, flexible funding mechanisms accessible to individual developers and globally distributed non-profits. However, the eligibility conditions may vary. For instance, the CBE JU encourages all stakeholders to apply, including SMEs, universities and local authorities, provided that they are a legal entity.[257]

European Digital Infrastructure Consortia

Just as EDICs have flexibility regarding the sources of funding, they may tailor the disbursement and oversight of funding, as determined by the statutes and other governing instruments such as the implementing rules to reflect lighter-touch administrative models. That may align with NGI-style cascade funding or participatory grantmaking mechanisms. Their design can include adaptive oversight frameworks suited to the open source ecosystem, which could be developed through the participation of community representatives and other experts in working or advisory groups.

In theory, the flexibility of this governance model means that funding recipients may include individual OSS developers and non-EU entities – a major advantage of this model. EDICs advance the general objectives and digital targets of the DDPP Decision at the EU level, such as 'promoting a human-centred, fundamental-rights-based, inclusive, transparent and open digital environment where secure and interoperable digital technologies and services observe and enhance Union principles, rights and values and are accessible to all, everywhere in the Union.'[258] While the EU must benefit, that value could arguably come from non-Europeans maintaining critical digital infrastructure projects upon which the EU depends. Likewise, EDICS may have Members who are 'third countries' if associated to 'a directly managed European Union programme that supports digital transformation of the Union and if its participation is necessary to facilitate the achievement of the general objectives and digital targets of the DDPP Decision' (emphasis added), as Article 4 of the EUROPEUM EDIC's statutes has permitted.

Important Projects of Common European Interest

IPCEIs tend to rely on national funding channels, each with their own bureaucratic requirements, and provide support to undertakings, understood in a broad sense to include companies,

organizations, and individuals co-investing in strategic projects. However, the design of IPCEIs is not well suited for OSS maintenance, which often involves distributed contributions and lacks the scale of private co-investment required. For this reason, while it is theoretically possible for individual maintainers or smaller non-profit entities to qualify as undertakings, in practice they face significant barriers in accessing this form of support. Additionally, while IPCEIs can, theoretically, be launched relatively quickly, asymmetries in availability of funding, coordination, and different disbursement timelines across Member States further complicate their effectiveness in addressing the needs of the OSS ecosystem.

Criteria #5: Community Focus

Joint Undertakings

JUs bring together a wide range of members in order to pool expertise, funding, and strategic direction across both public and private actors. For instance, the JUs established under Horizon Europe include the EU - represented by the EC - as well as participating states, founding members, and associated members. 'Founding members' are those research organizations, companies or countries that contributed to the JU's establishment and are directly listed in the Regulation. On the other hand, 'associated members' join the JU later signing a letter of commitment. Finally, 'contributing partners' are those countries or organizations that support the JU even without fully becoming members.

Furthermore, JUs typically develop fixed Strategic Research and Innovation Agendas (SRIAs).[259] These documents set long-term priorities, impact areas, expected outcomes and funding directions and are jointly shaped by industry, the EC, and research actors. While robust, these likely exclude smaller OSS actors, who lack the resources to engage with formal agenda-setting.

European Digital Infrastructure Consortia

The founding Member States may design EDIC governance to include advisory boards, working groups or participatory selection committees involving relevant ecosystem stakeholders (e.g., OSS maintainers, civil society, SMEs). This arguably enables iterative, tailored, collaborative and transparent funding decisions.

As considered appropriate, they could engage and convene relevant actors such as public entities, private entities, end users and industry, including as implementation partners, Members and/or expert advisors.[260] For example, the ALT-EDIC Statutes enable both a Scientific and Technical Advisory Board, and a Legal and Ethical Advisory Board. They 'shall be composed of experts in the fields relevant to ALT-EDIC, including, as appropriate, technical and scientific, as well as representatives of the user communities and other relevant stakeholder groups'.[261] For the EUROPEUM-EDIC, Members – in attending the Assembly of Members – may bring experts along, in accordance with the Implementing Rules.[262] It is reported that the CitiVERSE EDIC shall ' [a]ctivate a network of EU industrial partners, including SMEs, in Member States to provide technology capacity for the CitiVerse' and, through a Smart Cities Network, it aims to onboard around 100 cities by 2026 and develop a common platform.[263] Given the vast flexibility of the EDIC model, such examples are illustrative rather than exhaustive.

The type of stakeholders and kind of engagement that an EDIC offers externally may help to determine forthcoming support from EU projects. Indeed, out of the initial 38 proposals from Member

States for EDICs, DIGITAL elected to support a number, 'with a particular focus on industry-oriented projects'.[264] It is further notable that voting Members or Observers on the EDIC Assembly of Members could be diverse actors beyond purely Member States, including private or public entities. Yet, Member States retain the majority of votes.

Where the EDIC can receive diverse sources of support, including in-kind contributions, that could ease funding pressures and enable prioritisation of further impactful activities. However, there is a risk that founding Member States may have lasting (and even disproportionate) influence over the organisational structures, even if other Member States – and different stakeholders, where that is a possibility – subsequently join as Members. That depends on the Statutes in question, and whether they can be amended and under what circumstances. For instance, EUROPEUM-EDIC allows the Assembly of Members to amend the Statutes and Implementing Rules in certain circumstances, provided that a supermajority of two-thirds of Members present vote in favour.[265] For the ALT-EDIC, the Assembly of Members shall be responsible for, inter alia, 'amend[ing] the Statutes' (only the parts that the EC considers non-essential and in accordance with the procedures in Article 33 of the Statutes) and 'decid[ing] on any other matters that are necessary to fulfil the tasks of ALT-EDIC'.[266] Both suggest a degree of dynamism and flexibility in allowing the EDIC to evolve with strategic interests and approaches of the Members, although it remains to be seen how this works in practice.

Important Projects of Common European Interest

While the process has gradually become more transparent with the creation of the JEF-IPCEI,[267] project selection and prioritisation happen behind closed doors, often between national ministries and the EC. While broader ecosystem engagement – such as participation from OS communities, SMEs or smaller states – is possible in principle, this model typically does not facilitate it. It does not even allow for transparent deliberation on OSS dependencies. Consequently, funding priorities may underrepresent digital public goods, with priorities driven primarily by government-industry alignments rather than open ecosystem needs.

Criteria #6: Strategic Alignment

Joint Undertakings

As legal entities established under EU law, JUs align well with strategic goals like the Digital Decade, NIS2, or the CRA. They can explicitly incorporate legal mandates around CRA compliance, cybersecurity investment, and digital sovereignty into their governance statutes. For instance, JUs set up by Regulation (EU) 2021/2085 closely integrate with other EU instruments to 'develop close synergies with other Horizon Europe initiatives and other Union programmes [...] to reduce economic and social cohesion and reduce imbalances'.[268] Furthermore, they advance key EU priorities by investing in critical areas like 5G, AI, cloud, cybersecurity and green tech,[269] contributing to both digital and green transitions under the EU's broader policy agenda.

Assessment

- High alignment with regulatory frameworks.
- Easily anchored into MFF and EU digital policy strategies.

European Digital Infrastructure Consortia

Not only boasting a distinctive legal personality, EDICs can be designed to align with key policy goals and tailored implementation. Their inherent flexibility in what the Statutes may include could allow or encourage EDICs to work in close coordination with different EU regulations and institutions, including in the pursuit of cybersecurity (e.g. by contributing to the EU Vulnerability Database (EUVD) or supporting CRA compliance), while remaining adaptable to evolving regulatory and geopolitical landscapes. In fact, the EC has emphasised that EDICs may apply for funding under programmes relevant to its objectives and scope of activities, such as Horizon Europe.[270]

Broadly, reflecting on the EU-STF's potential to improve OSS cybersecurity, strengthen digital sovereignty and European competitiveness, there is clear strategic alignment with the EC's stated goals for EDICs as a novel implementation mechanism for digital coordination. That includes where EDICs contribute to 'reinforcing Europe's technological excellence, leadership, innovation and competitiveness in critical technologies'; 'addressing and solving strategic dependencies of the Union along the digital supply chains'; and 'increasing the availability and promoting the use of safe digital solutions'.[271]

Important Projects of Common European Interest

Because IPCEIs focus on industrial policy and state aid exemptions, they are less well-suited to fulfilling regulatory implementation functions. Their role is rather to support the EU's established priorities. As highlighted by the EC: "IPCEIs can underpin all policies and actions that seek to achieve common European objectives, in particular the European Green Deal, the Digital Strategy and the Digital Decade, the New Industrial Strategy for Europe and its update, the European Strategy for Data and Next Generation EU".272 However, once legal priorities have been set elsewhere, they can become useful instruments for delivering investment in strategically identified OSS dependencies by "bringing together knowledge, expertise, financial resources and economic actors throughout the Union and creating positive spill-over effects to the whole Union."[273]

Criteria #7: Transparency

Joint Undertakings

JUs are designed to ensure high levels of transparency and accountability through their formalised governance structure, which includes representation from the EC, Member States, and industry or research actors. Key decisions – such as work programmes, funding calls, and project evaluations – are typically published and subjected to public scrutiny, often supported by annual reports, independent evaluations, and performance audits.

However, the complexity and scale of JUs can occasionally dilute the clarity of decision-making for external observers. While formal procedures ensure traceability and openness in principle, the dense regulatory frameworks, technical language, and industry-heavy governance may limit accessibility and responsiveness to smaller or less-resourced stakeholders. Moreover, the high administrative burden and long timelines associated with JU processes may constrain more agile transparency practices.

European Digital Infrastructure Consortia

EDICs can be designed with strong transparency mechanisms, as the founding Member States

define their statutes, governance structures, and procedures. This could include open meetings, published work plans, participatory advisory boards, and public reporting beyond what is legally required. The degree of and mechanisms for transparency are therefore variable and highly customisable, but it depends on political will and the specific choices of the founding Member States in drafting the statutes.

Indeed, the statutes of two EDICs – ALT-EDIC and EUROPEUM-EDIC – illustrate such differences in approach. Under Article 23 of the ALT-EDIC Statutes, its proposed access to facilities for users 'shall be granted through a transparent procedure based on information provided through open electronic information taking into account the priorities, rules and conditions decided by ALT-EDIC'. In Article 26 of the EUROPEUM-EDIC Statutes, which also outlines the access policy for users, it emphasises the principles more than the procedures: 'Effective access to EUROPEUM-EDIC will be ensured based on open, transparent and non-discriminatory conditions'.

Both enable participation of trusted expert advisors and implementation partners. That said, different mechanisms abound, such as through a Scientific and Technical Advisory Board, and a Legal and Ethical Advisory Board (ALT-EDIC) or EBSI Technical Group (EUROPEUM-EDIC).

Important Projects of Common European Interest

IPCEIs are sometimes characterised by opaque decision-making, with project selection and funding priorities negotiated behind closed doors between national governments and the EC. Due to the lack of sufficient data on existing IPCEIs, it is difficult to assess whether public funds are being used efficiently or to evaluate the potential impact these projects may have on competition. Also, there is generally no formal obligation to disclose detailed processes, criteria, or rationales to the public or wider ecosystem. This can create challenges for aligning with open source and digital commons principles of openness and accountability.

Despite these concerns, recent best practices recommendations have been developed, within the 'Code of good practices for a transparent, inclusive, faster design and assessment of IPCEIs',274 aiming at enhancing transparency and openness in every stage of the process. For instance, recommendations concerning national calls for expression of interest emphasise that such calls should be open and widely publicised, with clear and detailed eligibility criteria, and transparent evaluation processes. Best practices also recommend holding information sessions prior to calls, in order to inform potential applicants about the application process and participation modalities. However, such best practices are not legally binding, and the implementation across Member States remains uneven.

5.3. Governance Setup Recommendation

In weighing the institutional options for the EU-STF, this study has done extensive legal and institutional analysis and considered a wide range of governance setups. In the end, we determined that hybrid/shared management structures offered the most promise, though each has their strengths and weaknesses. JUs offer legal robustness and long-term stability; IPCEIs are fast-moving and pragmatic; and EDICs are new but promising in their extensive flexibility and adaptability to a given context and involvement of relevant stakeholders.

We conclude that the most appropriate structure for launching and scaling the EU-STF is an EDIC, which the founding Member States can tailor for open source infrastructure investment and operate through a federated hybrid model. The fund must do more than administer grants; it must procure maintainers to do essential maintenance and development work, coordinate complex socio-technical ecosystems, and align national and EU-level digital priorities, all while earning the trust of a diffuse and deeply principled open source community.

There are significant advantages to a centralised EU-managed fund, particularly when it comes to attributing a dedicated EU budget line specifically for OSS maintenance and security. A directly managed programme would allow for clear budgetary earmarking and predictable multiannual funding, which is harder to achieve under an EDIC's co-financing model. There are weaknesses to the EDIC model, and careful attention must be given to how it is implemented and alongside whom. Governance could be labyrinthine and opaque, should the statutes favour that approach, and the vehicle is relatively nascent.

That said, the EDIC's flexibility enables a wide range of governance approaches, which may be amended in consultation with Members and stakeholders. Over time, if sufficiently funded and politically supported, the EDIC could also serve as inspiration for transitioning to a more centralised EU-managed fund.

5.3.1. Why an EDIC?

Both the centralised fund model and the EDIC model offer novel responses to the systemic market failures and strategic challenges Europe faces. The centralised model – either managed directly by the EC or through an agency like HaDEA – could deliver political visibility, coherence, and alignment with EU-level strategic goals. By treating open digital infrastructure as a public good deserving of coordinated public investment, a centralised EU-STF becomes a mission-oriented instrument to tackle systemic under-investment, reduce technological dependencies, and secure core digital assets.

However, the EDIC model better reflects the decentralised, collaborative nature of open source development. It allows Europe to build a flexible, resilient support structure that includes Member States, industry actors, and technical communities. This distributed governance logic supports autonomy and resilience by embedding capacity in national contexts while advancing a shared EU mission. While less high-profile than a centralised approach, an EDIC may be more responsive, legitimate, and durable in creating the long-term conditions for digital sovereignty through open innovation.

The most determinative advantage of the EDIC model is its legal and operational flexibility. It can be set up relatively quickly without requiring changes to legislation and can directly engage the open source and digital commons communities by partnering with national agencies, public-sector actors, OSS contributors, and other stakeholders. The recommendation of an EDIC does not mean a centralised approach cannot succeed, only that the former is more likely to deliver the impact expected from the EU-STF, at least in the short-term. The centralised approach offers the clearest institutional identity and sends a strong political signal, but the EDIC's distributed strength and tailored governance solutions give it the competitive edge.

5.3.2. Analysing the feasibility of the EDIC model

The EDIC model provides a legal basis for Member States and the EC to jointly establish and operate digital infrastructure projects, including where the founders may draw upon the strategic guidance of the EC in setting up an EDIC without imposing legal liability or responsibility. This is already being tested in the context of the proposed Digital Commons EDIC, and lessons from that experiment are directly relevant here. What sets the EDIC apart from the other models is its built-in flexible capacity for shared governance and pooled investment, without the bureaucratic weight or political sensitivities of creating a new EU agency. It is designed for the kind of flexible, infrastructure-oriented collaboration that the EU-STF requires, especially for something as horizontal and foundational as open digital infrastructure.

An EDIC may engage the private sector through various roles and mechanisms, such as by accepting contributions of financial support or in-kind contributions such as technology, infrastructure, or expertise. Private entities may participate as contributors, contractors, expert advisers or observers. They may even serve as voting Members, subject to the statutes of the EDIC.275 That said, Member States will always hold the majority of the voting rights, because where entities other than Member States are Members of an EDIC, they have proportionally less voting power.276 Nevertheless, the flexibility to engage private-sector actors in this way allows EDICs to draw on wider expertise and resources while ensuring that strategic control remains with the public sector.

Advantages of EDICs compared to JUs and IPCEIs

EDICs offer comparative advantages over other approaches. Unlike JUs, which demand a legislative act and typically take years to establish, EDICs can be set up more quickly through voluntary participation by Member States. Their design could allow membership and funding to scale and evolve dynamically, making them more adaptable to the political climate of 2025, where urgency around cybersecurity and digital sovereignty is growing but institutional consensus is still forming.

JUs bring institutional permanence and scale but are best suited to highly structured, industrially concentrated partnerships. Open source ecosystems are loosely federated, globally dispersed, and built on norms of openness and decentralisation. Attempting to fit a developer-led, community-centric domain into a rigid JU structure risks alienating the very people the EU-STF needs to engage, and the SRIA-driven governance of JUs is too slow-moving for the fast-evolving open source and security landscapes.

IPCEIs are a funding coordination mechanism, not a governance framework, and lack the institutional infrastructure to sustain long-term coordination of decentralised communities. They can unlock national co-financing for targeted projects and may complement the EU-STF in cybersecurity-critical dependencies, but they remain broadly top-down and ill-suited to the collaborative and iterative nature of open source development.

Cybersecurity frameworks can be more effectively embedded into the EU-STF through the EDIC model. An EDIC can be structured to interact with legislative frameworks such as the CRA and NIS2, cooperate with national cybersecurity agencies, and incorporate security audits and dependency mapping into its funding strategy. This would align regulation, public investment, and developer capacity

– a policy triangle no current mechanism fully coordinates.

The EDIC offers a viable path forward: its greater degree of flexibility than JUs and IPCEIs, as well as enables shared governance, pooled resources, and delegation of operational functions to a dedicated secretariat or coordinating body. It is well positioned to act as an enabling backbone for dynamic, long-term, and values-driven coordination. Crucially, it could contract out funding delivery to existing institutions with open source expertise (including, potentially, the German STF or its successor body), while maintaining strategic direction and oversight at the EU level.

A well-designed EU-STF EDIC must begin with a core group of willing Member States to act as founders, but have strong involvement from the EC – which we recommend a contribution at a minimum of EUR €350 million (likely earmarked or pre-validated through MFF negotiations – see below). Subject to the EC's approval of the EDIC, they could work with the EC and a coordinating entity, acting as the administrative and technical hub. This central node could be responsible for:

- Managing pooled funding and distributing it through low-burden, developer-friendly grantmaking (e.g., via cascade funding).
- Conducting or commissioning dependency analyses to identify critical OSS components, including by leveraging the CRA Administrative Cooperation Group (ADCO), which can request aggregated dependency analyses from market surveillance authorities pursuant to Article 13(25) of the CRA.
- Coordinating security audits aligned with CRA/NIS2 Directive objectives.
- Facilitating cooperation between national cybersecurity agencies, regulators, and funders in addition to relevant EU institutions and projects.
- Hosting an open governance process that includes representation from the OSS ecosystem (e.g. maintainers, civil society, industry, Member State liaisons, etc).

Importantly, the EDIC model allows for regional autonomy and participation by widening Member States, many of which may lack the resources to establish their own open source support structures. This federated governance structure would also mitigate risks of centralisation or Brussels-centricity, a concern voiced repeatedly in interviews and workshops. It also enables dynamic and gradual scaling, allowing Member States to join at their own pace while keeping the door open for future institutionalisation into a more permanent EU body, such as a JU or standalone agency – once the political and administrative groundwork has been laid.

Potential risks and challenges

EDICs are still relatively new, and there is limited precedent for one operating at this level of strategic ambition. Some interviewed for this study had negative experiences with their setup and delivery, raising concerns that an EDIC could become under-resourced or face coordination failures that undermine its effectiveness. These risks can be mitigated by creating a dedicated stakeholder advisory board with rotating representation from technical, civil society, and industry actors, and by using lightweight, interoperable reporting standards to avoid burdening OSS maintainers and small project teams.

The more fundamental risk lies in securing adequate and sustainable financing. None of the proposed governance or coordination measures can compensate for chronic underfunding. The EDIC should be explicitly linked to predictable and multiannual funding streams under the next MFF, potentially through a direct envelope in the European Competitiveness Fund and complementary support under the CEF. Member States should be encouraged to make national contributions, while pooled financing mechanisms – including voluntary industry co-funding and cascade funding through trusted intermediaries – could add flexibility and resilience. Without a clearly defined financial base, even the most well-designed governance framework will struggle to deliver on the strategic ambition envisioned for the EDIC.

5.3.4. Summary of recommendation

A EU-STF EDIC would offer the best institutional compromise between speed and legitimacy, EU-wide ambition and Member State engagement, and grassroots OSS culture and top-down strategic direction, providing a timely and tangible demonstration of EU leadership. It reflects a 'European way' of doing digital industrial policy, elevating community-based innovation to shared digital sovereignty goals with tangible applications for security, innovation, autonomy, resilience, and competitiveness.

The EDIC is the most flexible and best positioned for success in the current moment. While it may not offer the full industrial partnership model of a JU or the rapid scale of an IPCEI, it strikes the right balance of agility, inclusivity, and coherence to launch the EU-STF now, while leaving the door open for future evolution, continued coordination with the German STF, and similar Member State initiatives.

We recommend that the upcoming MFF – most notably the European Competitiveness Fund – set aside at least EUR €350 million to create a centralised standalone fund or serve as the minimum contribution to an EDIC. In the short-term, work should begin on setting up an EDIC, as it can provide strong EU-wide visibility and be operational relatively quickly, with the potential to evolve into more permanent institutional or federated arrangements over time.

5.4. Alignment with EU Legislation, Regulation and Institutions

Regardless of which model for an EU-STF is adopted, its compliance with EU legislation is not only legally necessary, but politically and economically desirable to further compliance, align with the regional bloc's common goals, and limit the prospects of fragmentation. This section firstly considers mechanisms for a potential standalone and centralised instrument. It then considers what implementation could look like via an EDIC, as well as maps relevant EU legislation and actors that it can coordinate with as part of that process.

5.4.1. Potential standalone and centralised fund implementation via HaDEA

A standalone EU-STF would fall under the direct management of the EC, most likely within DG-CNECT. However, in line with established EU governance practice, a large part of the executive and administrative implementation could be delegated to an executive agency such as HaDEA. Indeed, given its proven capacity in managing EU funds in the digital domain – including substantial components of Horizon Europe, DIGITAL, and CEF Digital – HaDEA would be a logical choice, especially

in the early stages of the programme.

5.4.2. Potential hybrid/shared management structure implementation via EDIC

Should it proceed under the EDIC model, the EU-STF shall be governed by EU law (especially the DDPP Decision and the EC Decision that establishes it), the law of the Member State where it has a statutory seat, and its statutes and implementing rules. That is both required by law, and consistent with the practice of existing EDICs.[278] Moreover, to maximise its impact and efficacy, the EU-STF should operate in full alignment with relevant EU legislation, supporting the implementation of the EU legal framework and contributing to the achievement of strategic policy objectives set up in key regulatory instruments.

In order to ensure that its activities are consistent with and complementary with the EU's broader regulatory strategy, the EU-STF should be explicitly aligned with the EU's goal of creating a harmonised and resilient digital governance framework, as exemplified and articulated by the NIS2 Directive, the AIA, the CSA and the CRA. For example, the NIS2 Directive (Article 1) aims to achieve high levels of cybersecurity across the EU by establishing obligations for public and private entities regarding risk management, incident reporting, and information sharing. The EU-STF can play a complementary role in supporting supply chain security through targeted investments in maintenance of critical OSS components; facilitating risk-management via proactive measures aimed at securing widely deployed OSS; and, more broadly, enhancing the open source components of essential digital infrastructures, thereby contributing to the EU's cybersecurity objectives in the NIS2 Directive.[279]

The AIA also has a key objective to enable the responsible development and deployment of AI systems across the EU. This must be done while ensuring that such systems are trustworthy, human-centric and aligned with EU values, as well as that they safeguard fundamental rights and mitigate threats from general-purpose AI models and high-risk systems. Another core objective is promoting an open, transparent and accessible development model, which includes development of open source general purpose AI (GPAI) models and software (Recital 102 AIA). The EU-STF supports both objectives by reinforcing compliant and sustainably maintained OSS infrastructure, funding transparent and values-aligned technologies, and lowering costs to foster safe experimentations (e.g., regulatory sandboxes) and fostering R&D.

Furthermore, the CRA aims to strengthen the EU's level of cybersecurity by enhancing Member States' and firm's capabilities and preparedness. This improves cooperation, information-sharing, and coordination among Member States and EU institutions, and helps to build EU-level capacity to complement national efforts, especially in the context of large-scale, cross-border cybersecurity incidents. The EU-STF contributes to these objectives. It not only funds the long-term maintenance of OSS, but also offers an institutional setting that fosters the cooperation between multiple stakeholders, including Member States and industry, thereby reinforcing both Member States' and the EU's responses to cyber threats.

The CRA, as important and novel legislation pending its partial application from late 2026, may offer emerging opportunities for the EU-STF to engage with new governance actors. It could provide specific expertise, ongoing monitoring of such incidents or other services as the authorities deem

appropriate and necessary. Relatedly, OSS stewards are obligated under Article 24 of the CRA to 'put in place and document in a verifiable manner a cybersecurity policy to foster the development of a secure product with digital elements as well as an effective handling of vulnerabilities by the developers of that product'. That policy shall particularly consider other dimensions that intersect closely with the EU-STF's remit, including promotion of 'sharing of information concerning discovered vulnerabilities within the open-source community.' Thus, OSS stewards and the EU-STF may cooperate in a mutually beneficial manner whereby they report vulnerabilities to the EU-STF, which may then take concerted action in securing the critical OSS infrastructure.

A further emerging avenue for engagement is the new Cloud and AI Development Act, which is part of the 'AI Continent' initiative. This proposed act is designed to address Europe's gap in cloud and AI infrastructure capacity through research and innovation to accelerate the greening of compute infrastructures and data centres for cloud and AI; facilitate private investment in sustainable cloud and AI capacity; and increase the secure processing capacity of EU-based cloud providers. Initial remarks of Henna Virkkunen, Executive Vice-President of the EC for Technological Sovereignty, Security, and Democracy, suggest that there may be space herein to consider coordinating open source efforts and investing in developer support – a role which the EU-STF could readily facilitate. However, concrete opportunities for engagement remain uncertain since the act was undergoing feedback and public consultation during the drafting of this study (June 2025).[280]

In navigating the EU regulatory and legislative framework, it is important to note that many legislative acts have carve outs for OSS and OSS components. That includes the AIA, CRA, revised Product Liability Directive (PLD), the Digital Content Directive (DCD).[281] In the case of the revised PLD and CRA, those carve outs include where OSS is developed and supplied for non-commercial purposes. Since various actors may not bear liabilities and responsibilities for OSS in certain contexts, they may pay further attention to the mandate of the EU-STF and its impact on securing software supply chains.

Meanwhile, the next Framework Programme for Research and Innovation (FP10)[282] could support upstream research and innovation that feeds into the deployment-focused work of the EDIC, fostering synergies without overlapping mandates. The EU-STF could further engage with other relevant actors, including in the cybersecurity space, such as the EC-OSPO, national level OSPOs and national cybersecurity agencies. An EU-STF EDIC could reinforce the idea that security is not an external compliance obligation but a core part of infrastructure investment. In this way, it aligns the dynamic intersecting parts of regulation, public investment, and developer capacity.

5.5. Implementation Requirements

In order to create and implement an EU-STF EDIC, the process involves three important steps. Firstly, mobilisation of at least three Member States – who must provide sufficient funding and decide upon essential elements of the EDIC's statutes prior to seeking the EC's approval (e.g. whether the statutory seat shall be, and duration). Secondly, the EC must approve their request via a formal decision-making process in accordance with Article 15 of the DDPP Decision, including once they considered general objectives (Article 3) and as well as the 'purposes and goals' of the MCP. Finally, there is entry into force and implementation of the EDIC.

This section focuses upon that final stage, specifically offering legally-based guidance and practical suggestions as to how the EU-STF can be operationalised. It assesses how to: (1) operationalise the EU-STF as a mission-driven fund through coordination with actors beyond EU agencies, especially when coordinating with the German STF; (2) attract funding and disperse it effectively across the five types of activities detailed above; and (3) enable an appropriate level of dynamism and flexibility in the governance arrangements as the landscape and actors evolve, and the functional processes and decision-making behind projects are refined for maximum value add and impact.

5.5.1. Coordination with the German STF and other non-EU stakeholders

A key question for the EU-STF's design and implementation is how to meaningfully engage different stakeholders beyond those from the EU above. This must be done in particular with the German STF, as it is the most closely aligned entity in terms of its overall mission, methodologies and target audience. But how could the EU-STF retain its institutional autonomy and distinctive identity whilst respecting that of the German model?

Again, the significant flexibility of the EDIC statutes means that they could expressly provide for the German STF to collaborate with the EU-STF as its close strategic partner, advisor and even as a Member or Observer in the Assembly of Members. The DDPP Decision permits all above options. Indeed, the German STF may become a Member or Observer in its own right, although potentially with a proportionally lower vote in the former case, since Member States are mandated to retain the majority of votes.[283] Alternatively, a Member State (e.g. Germany) may choose to be represented in the Assembly of Members by one or more public entities, including 'private entities with a public service mission'.[284] That category encapsulates the German STF.[285]

Generally, the constitutive governance documents of legal entities tend to create a designated 'class' or 'category' of actors (e.g. international organisations with a European interest, or private entities with a public service mission, to invoke practice of current EDICs). These are actors who can undertake a certain role and fulfill certain responsibilities, be it as a voting member, observer, expert stakeholder, donor, etc. That means that if a given actor becomes redundant, closes, and/or has serious governance issues, the primary entity is not automatically beholden to keeping it, which would be more challenging (but not necessarily impossible) if it was included by name. Nevertheless, it is certainly possible that the EU-STF EDIC's statutes could name the German STF to perform a specific function within or in close partnership with it, subject to the preferred approach of the founding Member States at least at first, and then potentially of the Assembly of Members if the statutes and implementing rules are amendable.

A variety of different models are available for managing a close strategic partnership, without alternating the legal form of the EU-STF and the German STF. The former's statutes and implementing rules may expressly provide for such a cross-border collaborative governance arrangement. Options include a Contractual Joint Venture (where parties remain legally independent unlike Equity Joint Ventures, but they share a standing cooperation agreement); a Memorandum of Understanding (depending on the terms and conditions, this can be non-binding, partially or fully binding); or a Strategic Alliance (for longstanding partnerships, with possibilities including co-branding, shared resources, and joint applications for funding). An agreement could also cover several relevant considerations, such as:

defining each entities' respective role, funding responsibilities, and project deliverables; the choice of governing law; and agreed dispute resolution mechanism (e.g. arbitration).

Regardless of the instrument that is preferred, both the EU-STF and German STF would need to comply with EU law. This encompasses competition law, data protection regimes including the GDPR, procurement rules (if public entities or funds are involved) and tax (which depends on both the state disbursing the funds and the eventual host state/their own taxation rules).

A broader question is how the EU-STF EDIC could have a distinctive identity, which is not necessarily subsumed by the interests and priorities of the founding Member States. They must permit participation of all Member States on fair and reasonable grounds throughout the duration of the EDIC. However, it is discretionary whether they permit other actors to fulfill any number of governance and implementation functions. For this important initiative to succeed, they should do so in a manner tailored to and befitting the open-source model and the scale/urgency of the challenge. Lessons – whether positive or negative – may be drawn from the approach of the two most thematically similar proposed EDICs, namely the Digital Commons EDIC and CSC-EDIC. At least one EDIC, the ALT-EDIC, has been far more restrictive in the decision-making powers of other actors – only Member States can vote in the Assembly. That presumably comes from the founding Member States wanting to consolidate their power.

In summary, the very flexible nature of EDIC statutes means that an EU-STF could theoretically engage in a strategic partnership or another arrangement with the German STF. This could be done in a tailored manner that respects and retains their distinctive identities while delivering more effective and efficient outcomes for funders and stakeholders in the open source ecosystem.

5.5.2. Pooled funding and disbursement

Precise modalities for pooling and then disbursing the EU-STF's funding could likely be dealt with through flexibility in the statutes and, if available, the implementation rules and procedures. In seeking localised implementation partners, the LDT CitiVERSE EDIC has adopted a Smart Cities Network, and aims to 'onboard about 100 cities within two years and develop a common platform for Local Digital Twin technologies'.286 While granular details of this funding model are unclear, each participating Member State will have to appoint their national coordinator,[287] perhaps implying that funding is dispersed at least in part locally, and partly matched by the national or local authorities.

A critical question arises of whether the EU-STF would strategically disperse its funding through other vehicles. This could be, for example: (1) national or other geographically defined hubs, thereby directly funding recipients who are 'based' in the EU/EEA, and then potentially having a default hub for those further afield, assuming that such recipients are eligible, as they are under Germany's STF;[288] (2) specific bodies/partners depending, for instance, on the type and/or location of the relevant activity covered; or (3) a centralised hub, presumably but not necessarily within the host State.

The transboundary nature of OSS projects would lend itself to having a disbursement plan encompassing maintainers who are based beyond EU/EEA borders, as the German STF has done. Limiting funding opportunities to maintainers based in the EU/EEA would dramatically reduce the

impact of an EU-STF, as the geographical location of the maintainers has no bearing on whether a particular OSS component forms part of Europe's critical open digital infrastructure. When it comes to mapping and identifying OSS dependencies and projects of strategic interest, the EU-STF could explore delegation or coordination with other relevant stakeholders, such as the EC-OSPO as they cover OSS dependencies in public administration to some extent. On cybersecurity, there is potential to coordinate with the CSC-EDIC (if successfully approved) including on security training.

5.5.3. Dynamism and flexibility in the governance arrangements

As the previous sections have emphasised, an attractive feature of an EDIC is its flexibility – although the ability of non-founding Members to amend the statutes and implementation rules (and the manner in which they do so) is not guaranteed. For instance, EUROPEUM-EDIC allows the Assembly of Members to amend the Statutes and Implementing Rules in certain circumstances, provided that a supermajority of two-thirds of Members present vote in favour.289 For the ALT-EDIC, the Assembly of Members shall be responsible for, inter alia, 'amend[ing] the Statutes' (only the parts that the EC considers non-essential and in accordance with the procedures in Article 33 of the Statutes) and 'decid[ing] on any other matters that are necessary to fulfil the tasks of ALT-EDIC.'290 Both suggest a degree of dynamism and flexibility in allowing the EDIC to evolve, whether to accommodate different Member priorities, shifting actors or mechanisms for realising their strategic aims.

VI. Call-to-Action: Operationalising the EU-STF

The process of conducting this feasibility study has revealed deep pockets of political will and momentum for the establishment of an EU-STF. Given our knowledge of the geopolitical trajectory of the next 5-10 years, as well as the groundswell of support for digital sovereignty, Europe now has a vital opportunity. Now is the time to act decisively by investing at the most fundamental parts of our digital society: open digital infrastructure.

The establishment of an EU-STF would, if implemented in line with the German STF, represent a transformative step towards operationalising Europe's digital policy ambitions. The German STF succeeded in providing targeted, long-term funding for critical open digital infrastructure focused on foundational open source technologies that underpin digital sovereignty, cybersecurity, and competitiveness. The EU-STF would build on this, renewing the focus on security and enabling a scope of investment and industrial coordination which is essential for a continent-wide effort. To this end, the EU-STF is envisioned as a scaled-up, pan-European initiative with a proposed EU funding contribution of at least EUR €350 million (we consider this a lower bound) to invest in the maintenance, security, and improvement of key ODBTs (open digital base technologies), as well as help identify and map dependencies and invest in ecosystem strengthening activities. It would support digital sovereignty, but more concretely aim to reinforce five key policy objectives essential for a grounded version of digital sovereignty: security, innovation, autonomy, resilience, and competitiveness.

The EU-STF can extend the German STF's strengths – community engagement, flexibility, and transparency – while adding stronger coordination with cybersecurity priorities, industry collaboration, and pooled financing to align with Europe's digital sovereignty and industrial policy objectives. If implemented successfully and with the right level of ambition, it would reduce strategic dependencies, improve understanding of and response time in cybersecurity, enable the re-shoring of innovation capacities, bolster domestic industry and SMEs, and reinforce Europe's control over its own software supply chains. Building on a proven model and well-known brand, the EU-STF would have a jumpstart as an initiative.

The EU-wide fund would constitute a structural transformation in digital investment in Europe. Chronic under-investment in OSS creates systemic risks – exposing Europe to cybersecurity threats, supply chain vulnerabilities, and strategic dependencies on non-European technology providers. This draws on the logic of Europe's digital political economy, showing how mission-driven, collective investment in open digital infrastructure addresses market and system failures that the private sector alone cannot fix. The EU-STF is positioned as a cost-effective, strategic multiplier: a means to secure the open source ecosystem, reduce dependency on foreign technologies, and foster innovation and economic growth aligned with European values and interests. It would serve as a dedicated, mission-driven investment vehicle, pooling resources across Member States and industry to protect and sustain Europe's open digital infrastructure.

Based on extensive interviews, we determined that policymakers should ensure that the EU-STF is designed as more than just another funding vehicle. It must embody the principles that have made the German model successful, while scaling these to a European level:

- **Pooled financing** refers to a mechanism where Member States, EU institutions, and potentially private partners contribute to a common fund dedicated to supporting open source projects critical for Europe's digital infrastructure. In this way, it is a public-led intervention while not solely being reliant on public financing.
- **Low bureaucracy** to make funding accessible to open source maintainers and community-driven projects.
- **Political independence** that empowers Member States and engages the open source ecosystem, while avoiding unnecessary centralisation.
- **Flexible funding**, including cascade funding and milestone-based grants, that can respond to both long-term maintenance needs and urgent security challenges.
- **Community focus**, ensuring legitimacy and trust among stakeholders while enabling accountability of the fund and buy-in from across the open source ecosystem.
- **Strategic alignment** with EU policy objectives, notably the Digital Decade targets, the CRA, and broader efforts to enhance Europe's cybersecurity posture.
- **Transparency** in funding decisions and governance, ensuring legitimacy and trust among stakeholders while allowing for enhanced scrutiny and oversight.

Operationalisation requires concrete steps to embrace these principles and help unlock. In closing, we propose three distinct pathways to fund and operationalise the EU-STF, each grounded in different governance and legal frameworks. These models differ not only in scale, but in their institutional logic, administrative complexity, and capacity to meet the core objectives of the EU-STF – namely, to fund critical open source infrastructure, foster cybersecurity, and support digital sovereignty.

6.1. Budget Categories for Implementation of the EU-STF

6.1.1. Option #1 – 'The Moonshot Model': Standalone and Centralised Fund (at least EUR €350 million over 7 years)

'The Moonshot Model' – Institutional Strength, Political Visibility, Strategic Coherence

The most ambitious model proposed is the creation of a standalone, centralised fund underpinned by a dedicated legal mandate and allocated a budget of at least EUR €350 million over a seven-year period. This funding would be secured through the EU's MFF and either set up within an executive agency like HaDEA or delegated to a new executive agency. It would represent a bold institutional step forward in treating open digital infrastructure as a strategic priority on par with energy, defence, or semiconductors – an instrument that not only funds software maintenance, but symbolises Europe's commitment to security, innovation, autonomy, resilience, and competitiveness.

The core advantages of this model lie in its clarity of purpose, centralised oversight, and ability to enforce alignment with the EU's strategic and legal objectives for digital policy. By consolidating strategic direction and disbursement in one structure, the EU-STF could maintain focus on systemic

investment gaps in OSS infrastructure, manage risks related to cybersecurity vulnerabilities, and integrate funding priorities across public and private sectors. Such a structure could also facilitate oversight, reduce duplication, and ensure coherence across Europe.

Yet, these strengths come with significant structural and political trade-offs. The feasibility study highlights the considerable setup time and complexity of securing MFF funding, particularly given the tight budgetary environment and competition with other EU priorities. A centralised fund risks becoming overly bureaucratic, less responsive to the distributed and iterative nature of open source development, and politically vulnerable to changing EC priorities. Moreover, while the fund might be operationalised by an executive agency like HaDEA, this presents further limitations. An executive agency like HaDEA is well-versed in digital and health domains but lacks tailored mechanisms for community-centric, developer-friendly funding, and is unlikely to enable the low administrative burden and participatory processes that OSS ecosystems demand. Its centralised procedures may also stifle bottom-up innovation and limit the fund's ability to reach more grassroots or under-resourced OSS maintainers.

In summary, this 'moonshot model' offers high strategic clarity but suffers from operational rigidity, cultural mismatch with the open source ecosystem, and significant political risks. It is aspirational, but also potentially fragile if it is not designed well, given a strong mandate, and coordinated closely with existing legislation and regulations. This requires strong buy-in from the EC; weak or tentative buy-in risks not producing the intended impact.

6.1.2. Option #2 – 'The Pragmatic Model': EDIC (EC, Member State, and Industry Co-Financing) (at least EUR €350 million from EC)

'The Hybrid Model' – Ecosystem-Aligned, Relatively Fast to Launch, Politically Flexible

A more decentralised, hybrid model centres the EU-STF around an EDIC funded entirely through voluntary contributions from Member States and possibly the EC, as well as (where permitted) private sector or philanthropic partners. Unlike Option #1, this version does not assume a direct EU budget line, though the EDIC may later apply for EU grants, receive funding from the EU, or coordinate with EU programmes. It is possible for funding to be 'earmarked' as part of an existing budget line that would then go on to fund the EDIC.

This model perhaps more closely preserves some of the spirit and institutional logic of the German STF. It offers a high degree of agility, low political overhead, and deep alignment with the collaborative and decentralised nature of open source development. It also avoids the need for legislative change or onerous MFF negotiations, as the work to set it up can begin immediately. This allows it to be launched quickly, potentially even in parallel with discussions on a more centralised or hybrid model. Again, while the MFF negotiations are not necessary for establishing an EDIC, the current MFF negotiation process (as of July 2025) could set aside funds via programme budgets to directly contribute into this fund to significantly amplify its reach and impact.

Crucially, the ability to finance EDIC activities from existing programme envelopes avoids many of the political complexities associated with creating a new fund. There is no requirement to open new negotiations within the MFF, no need to pass enabling legislation, and no disruption to the current financial architecture of the EU. The EC retains its strategic oversight and financial controls, but within a

more modular, responsive governance framework. Unlike with the standalone and centralised fund, the EC may contribute financially or in-kind to an EDIC using existing funds from current EU programmes, provided that the EDIC's objectives align with the priorities of those programmes. EC contributions typically draw from established programmes such as DIGITAL, CEF Digital), or Horizon Europe. This makes the EDIC a politically and fiscally pragmatic vehicle, well-suited to the constraints and urgency of the 2025 policy context.

The strengths of this approach are compelling when compared to the standalone and centralised fund. It would be comparatively easier to get off the ground quickly and flexible to EC contributions over time, requiring less of an upfront commitment in 2025. An EDIC could be designed to enable tailored funding mechanisms (e.g., cascade funding, developer-friendly grants, low-burden maintenance support, etc), while possibly creating space for distributed governance. This would create room for more open calls, community participation, and encourages Member State ownership and coordination. It can also provide space for the involvement of trusted intermediaries (such as the German STF) in implementation or fund disbursement, preserving continuity and community trust. It would be essential for the EDIC to have core staff that mirror some of the roles taken by the staff of the German STF.

However, this model also faces significant limitations, especially in terms of scale, visibility, and coherence. Without a significant upfront commitment at the EU-level, there is a risk that the fund remains underfinanced or unevenly financed, limiting its power and mandate. This depends in large part on the political will and fiscal capacities of contributing states, as well as how the EC chooses to engage with the EDIC and whether industry sees this as a useful vehicle to contribute into. Participation from industry may also be limited unless carefully structured, given that private entities cannot be voting members in an EDIC and may lack incentives to contribute without governance involvement. As a result, an EDIC-only model may struggle to create EU-wide visibility or branding, especially if Member States dominate the agenda or if no central secretariat provides cohesion. Coordination with broader EU policy goals – such as CRA compliance, implementation of proposed legislation like the Cloud and AI Development Act, and the delivery of digital sovereignty policies – may depend on informal relationships rather than institutional mandates.

In short, the EDIC-only model likely offers a realistic short-term pathway and the best cultural fit for the open source community, though it may be constrained by its reliance on voluntary contributions and limited political weight. Nevertheless, the architecture could be attractive to the EC in particular because it enables them to act with institutional flexibility, and for the vehicle to adapt over time without a significant upfront investment and then a long implementation lifecycle. This makes the EDIC model particularly attractive in a context requiring incremental institution-building, and coordination with the German STF (and potentially other bodies set up in other Member States).

6.2. Strategic Recommendations

To ensure the successful uptake of the EU-STF feasibility study and the realisation of our call-to-action, the challenge is to get the details right. Policymakers and others invested in a successful outcome of this study should consider the following strategic recommendations across four key categories, including recommendations for each budget category and a section focused on cross-cutting recommendations. These recommendations build on insights provided during the interviews

conducted during this study.

6.2.1. Strategic design and setup of 'The Moonshot Model'

Recommendation #1 – Policymakers should attempt to secure strong political buy-in and clear legal mandate for the EU-STF through the upcoming MFF negotiations:
The 'Moonshot Model' can only succeed if it is backed by robust political commitment and an unequivocal legal mandate that frames open digital infrastructure as a strategic EU priority, comparable to energy, defence, or semiconductors. Without such buy-in, the long and politically sensitive process of negotiating MFF allocations risks diluting the fund's scope, delaying its implementation, or rendering it ineffective. Given that the fund would need to be anchored in the next MFF, early negotiations must position it as part of Europe's broader industrial and security strategy, ensuring its inclusion in the strategic priorities agreed by Member States and the European Parliament. This will require coordinated advocacy during the MFF revision and programming process to secure a dedicated budget line, possibly as part of the broader European Competitiveness Fund, and protect it from competing political priorities. That said, while the centralised nature of this model offers strategic clarity and coherence, these benefits will only materialise if the fund is designed and defended at the highest political level as a critical instrument for Europe's digital sovereignty, security, and competitiveness. Negotiators should therefore treat the EU-STF not as a discretionary digital initiative but as a core component of Europe's industrial and security strategy. Weak or tentative support would likely lead to bureaucratic inertia, cultural misalignment with the open source ecosystem, and failure to address systemic investment gaps, undermining the very strategic objectives this model seeks to achieve.

Recommendation #2 – Policymakers should create mechanisms for streamlining administrative processes in the design of the vehicle: Administrative simplicity is essential to reduce friction for maintainers and developers. Lessons from the German STF highlight the importance of minimising bureaucratic burden to accelerate disbursal and facilitate participation, particularly from volunteer-driven or small-scale open source projects. Projects must be able to apply to the agency regardless of their place of residency or establishment, and funding cannot simply be decided from the top-down. The cascade funding programme of the NGI is an important consideration in this regard. Anything else would be against the spirit of the original German STF. People interviewed for this study most frequently expressed this desire as something that must be preserved in an EU-STF. The open source community is uncomfortable with administrative burdens given the lack of adequate funding and support presently, especially given the volunteer basis by which a notable proportion develop open and collaborative software. Introducing high levels of EU/EC bureaucracy into the application and reporting of project funding requests would hinder funding reaching the open source ecosystem.

Recommendation #3 – Policymakers should guarantee a degree of fund independence from the EC, but with strong alignment with shared EC and Member State priorities: A balance must be struck between the priorities and engagement of Member States and alignment with the larger digital policy ambitions of the EC, as outlined in the section on digital economy. As Section V outlines, excessive centralisation could delay implementation and discourage Member State and community engagement, while strategic alignment with EU digital sovereignty and cybersecurity goals remains critical for ensuring coherence and non-duplicative balance. Given the inherent tension that might arise from a joint/hybrid vehicle, this tension must be carefully managed by the founding stakeholders of the EU-STF.

Recommendation #4 – Policymakers should develop oversight mechanisms that are suitable for open source development: Traditional oversight models may not reflect the decentralised and transparent norms of the open source community. Oversight mechanisms must recognise the unique dynamics of open source ecosystems – while ensuring accountability, impact, and legitimacy in how public money is used. This will be vital for the success of the EU-STF, partly because the German STF has had so much success in doing this already. Introducing a new level of complexity and opaqueness due to the EU-STF being a 'European fund' would be ill-fitting, though possibly remedied by the creation of vehicles that could channel funds into national, regional, and local ecosystems, supporting diverse strategic interests.

Recommendation #5 – Policymakers in the MFF negotiations should earmark corresponding investments for mapping dependencies (via Horizon Europe and the next research framework programme) and ecosystem strengthening activities (via the EU Competitiveness Fund): While this report has recommended an EDIC or other joint structure, part of its funding should be allocated via the upcoming MFF negotiations, which are negotiated between the EC and European Parliament. Based on the structure of the current MFF, our landscape review recognises that the Horizon Europe framework could support the research-intensive work of software dependency mapping, while the CEF Digital can provide the kind of public infrastructure support – e.g., training, cross-border collaboration platforms, or security testing infrastructure – needed to reinforce open source ecosystems. These efforts could be initiated in parallel to a decentralised (or even centralised) fund's setup to ensure there is actionable data and absorptive capacity when the first calls are launched, though it does not preclude the fund also implementing similar or complementary activities. The EC should incorporate further synergies with open source maintenance funding in the new MFF package and its accompanying sectoral proposals.

Recommendation #6 – The EC should commission an initial mapping that can inform prioritisation of funding across the areas identified in this study for the first round: Dependency mapping is essential to know where to direct initial investment for highest leverage. It is one of the essential foundational enablers for the EU-STF to be both strategic and effective at a continent-wide level of ambition. As the report outlines, without a clear view of where open source dependencies lie in critical European infrastructure, or what structural gaps exist in the ecosystem, investments risk being scattershot and not achieving the intended scope and ambition of having an EU-wide version of the STF in the first place. A dependency mapping should focus on upstream components and foundational technologies that underpin broad swathes of EU infrastructure, with implications for cybersecurity, competitiveness, and resilience. Again, it does not preclude further research being conducted through the Horizon Europe programme or being funded by the EDIC itself.

6.2.2. Strategic design and setup of 'The Pragmatic Model'

Recommendation #1 – The founding members, partners, and/or supporters of the EU-STF should encourage Member States to set up their own vehicles to support disbursal of funds, and work closely with the German STF (at least at first): A hybrid EDIC model relies on distributed but aligned implementation. Encouraging Member States to create national, regional, or local funding structures – akin to the German STF – helps localise investment, build administrative capacity, and deepen ecosystem engagement. These national vehicles can tailor support to domestic needs while remaining coordinated through the EU-STF's central governance, ensuring cohesion without centralisation. A

hybrid EU-STF model is only viable (and arguably most effective) if complemented by national-level institutions, or by a company model like the German STF being set up in Brussels or elsewhere as the de-facto standard. That said, particularly at first, a more federated approach – encouraging Member States to establish aligned vehicles (as Germany has with the STF/Sovereign Tech Agency) – can strengthen the overall ecosystem, expand capacity, and enable regional experimentation while maintaining coherence under the EDIC framework. Initially, this could mean contributing more money into the German STF, rather than having the fund do all disbursal of funding on its own.

Recommendation #2 – EC policymakers interested in the EDIC should work with Member States to identify significant upfront commitments before implementing this model: Securing political and financial buy-in early is essential. This study has emphasised that broad and early Member State commitment is a prerequisite for its feasibility, ensuring that the fund is not a top-down imposition but a cooperative effort. Without this step, subsequent governance or design actions may falter or be undermined by lack of participation. This must also extend to material and demonstrable financial commitments which help meet the threshold of funding identified previously. Significantly less would risk undermining the objectives of having such a fund in the first place.

Recommendation #3 – The founding members, partners, and/or supporters of the EU-STF should ensure broad and representative buy-in for the EDIC from Member States from the beginning: Closely tied to upfront commitments, this step guarantees that Member States feel ownership over the EU-STF's vision and institutional setup. As the EDIC model is proposed for its flexibility and shared management structure, early representation ensures strategic direction and funding alignment across diverse interests. While it is unreasonable to expect all EU Member States to buy-in, it should include representatives across EU regions and include countries of different sizes, and with different voices and interests. Simply allowing this to be an effort driven by France and Germany, like many other digital policy projects, would not effectively position it for success. We argue that the buy-in of frugal states such as the Netherlands, Austria, Sweden, or Denmark, who normally advocate for limited spending and strict budget controls in the EU,[291] would constitute an early positive signal for the feasibility of this effort.

Recommendation #4 – The founding members, partners, and/or supporters of the EU-STF should enable coordination of the EDIC or joint structure with the German STF: The German STF provides the operational blueprint and credibility for the EU-STF, and the design of the EU-STF must not veer too far from what has already been successfully achieved while scaling up and supplementing those efforts, including in cybersecurity. Close coordination with what has been done before ensures continuity, scalability, and coherence across governance levels, avoiding redundant structures and leveraging the Sovereign Tech Agency's existing expertise, as strongly recommended in Sections IV and V. It will also allow the German STF to serve as an effective vehicle for channeling EDIC (or other joint structure) support until such a time as there is a plurality of institutions in Member States to help administer such funds.

Recommendation #5 – EC policymakers and Member States should ensure that the design of the EDIC or other joint structure allows its statutes to evolve over time, and make sure it enables industry co-financing: Given the evolving nature of open source and digital infrastructure needs, flexibility is key. The governance setup must permit iterative statutory changes to adapt the fund's scope and implementation tools to emerging challenges without legal or bureaucratic bottlenecks. The EDIC,

for example, has a lot of flexibility in terms of what can be included in the founding constitutive document, provided it ticks off certain minimum features and legal requirements. However, it would be incumbent on the original Member States founding the EDIC to enshrine coordination mechanisms (or the possibility for their introduction) into its statutes (and, where necessary, its implementing rules). Careful attention must be given to whether/how that constitutive document could change – including as Member States join, as priorities and structures shift, as well as how industry members can contribute in and participate related to co-financing.

Recommendation #6 – EC policymakers and Member States should extensively consult European industry on the needs and requirements for co-financing of an EDIC: Private sector co-financing is not just desirable – it is vital for long-term sustainability. The EU-STF must align with industrial policy goals and listen to firms' needs, especially regarding strategic components they depend on. Co-investment also increases legitimacy and adoption of the vehicle, but it's important that this is built-in from the outset and not designed as an afterthought. This emerged quite clearly through this study as a key design feature of the EU-STF, The flexibility of the EDIC could accommodate this in theory, subject to how the founding Member States design the statutes. Accordingly, private co-financing of EDIC activities can be effectively unlocked and marshalled towards the strategic objectives highlighted above.

Recommendation #7 – Member States should focus on foundational and critical components from the outset, and identify a funding amount that scales on that over time: From the start, the EU-STF must prioritise open source components that are foundational digital infrastructure to Europe's public services, industries, and critical sectors such as healthcare, energy, and transport. As referenced before, these are generally the 'upstream' technologies – e.g. libraries, protocols, cryptographic tools, package managers, and operating system components – on which many 'downstream' applications depend, and thus one to several layers down. The study has emphasised that disruption to such components can have cascading and catastrophic effects, as shown by past incidents like Log4Shell. Therefore, initial funding must be directed to those components with the greatest systemic importance and vulnerability. It is important that a commitment to the most foundational components, identified through research and analysis, be prioritised as part of the first round of the EDIC's activities to demonstrate impact. This can still be supported by an open call.

Recommendation #8 – The founding members, partners, and/or supporters of the EU-STF should work with the German STF on early project identification and disbursal of funds: As the report notes, the German STF has already developed clear selection criteria and a pipeline of vetted, high-impact OSS projects. Rather than duplicating efforts or delaying disbursement through a lengthy ramp-up phase, the EU-STF should collaborate directly with the German STF in the early stages to identify and fund projects using its mechanisms and community relationships. This approach helps build credibility for the EU-STF by showing quick, tangible impact while simultaneously allowing its own internal capacity – staffing, oversight systems, funding typologies, etc – to be built out. It also ensures that European taxpayers see a return on investment early in the fund's life, which is crucial for political and public legitimacy. Leveraging the German STF's existing project pipeline and selection methodologies reduces ramp-up time and risk. This 'borrowed capacity' can ensure rapid first-round disbursals while the EU-STF builds its own institutional infrastructure, while also helping to act as a supporting vehicle for the EU-STF in the period while it is still being conceptualised and set up, and after its initial implementation.

Recommendation #9 – The founding members, partners, and/or supporters of the EU-STF should support the diversification of funding architecture as the EU-STF scales: While the EU-STF will likely index towards Member State contributions at first, it must be scalable. It should begin with a strategically chosen set of high-impact interventions, but it must also have a funding architecture and institutional mandate capable of expanding over time – whether through the MFF, national co-financing, or matched industry contributions. This scalability and flexibility ensures the fund remains responsive to funding Europe's evolving digital policy goals – such as CRA compliance, AI sovereignty, and industrial resilience – as well as prioritising areas identified by the open source ecosystem itself. To reduce risk and increase resilience, the fund should promote hybrid funding models involving private, public, and philanthropic actors. This also helps sustain projects beyond EU-STF grant timelines and encourages broader participation in funding OSS.

6.2.4. Cross-cutting recommendations

Recommendation #1 – Champion urgency by advocating for the broad benefits of an EU-STF: The study makes clear that Europe faces a critical window of opportunity: systemic risks in open digital infrastructure are rising, and reactive funding efforts will be too little, too late. To galvanise action, policymakers must communicate that the EU-STF is not a niche initiative, but a foundational investment in Europe's digital autonomy, economic resilience, and security. Policymakers should start talking about open source as open digital infrastructure, building on the understanding in this study. They should also present a clear, unified message – grounded in data and real-world vulnerabilities – that an EU-STF is needed and differs from other digital or tech sovereignty initiatives.

Recommendation #2 – Consider calls for adjacent but unrelated investments, and counteract them with a clear policy argument: As the fund gains visibility, it will attract interest from diverse actors pushing unrelated priorities under its banner. To safeguard coherence, policymakers must defend a clear mandate for the EU-STF – focused on mission-driven investment in open digital infrastructure with high public value and systemic relevance. This means resisting 'mission creep' and reinforcing that the fund's legitimacy derives from addressing well-documented gaps in critical open source funding. Policymakers must proactively communicate what the EU-STF is (and is not), using strong, values-based policy arguments to resist pressure for unrelated or diluted investments. Those who wrote this study are available to help in such efforts.

Recommendation #3 – Actively involve European industry in the design and set-up of the fund: Industry is both a major beneficiary and a critical enabler of open source sustainability – an idea that this study has helped re-center. Engaging leading European companies and getting them bought into the strategic importance of the EU-STF addresses strategic industrial dependencies, encourages co-financing, and can support common shared objectives. Digital sovereignty is about choice, so it is not the technology as such that is sovereign or not, but whether countries, companies and individuals are empowered to use and design them independently. Involving industry early on builds on the momentum while focusing the energy towards a targeted goal that supports the rest of their ambitions: open digital infrastructure investment.

Recommendation #4 – Coordinate strategically with existing initiatives like EuroStack and OIS to ensure a strong and well-differentiated policy offering: Strategic coordination with peer initiatives avoids redundancy and strengthens the EU-STF's unique position in the policy landscape. EuroStack focuses on sovereign infrastructure and industry mobilisation, while the OIS proposes open, modular tools for public services. The EU-STF should not compete with these efforts but instead complement them through focused investments in shared open source infrastructure, supported by a distinct governance and funding approach. Strategic coordination will prevent confusion, leverage shared momentum, and ensure a cohesive message to industry, Member States, and civil society.

Recommendation #5 – Explore investments in large-scale projects of strategic interest: While the core mission of the EU-STF is to shore up foundational open digital infrastructure, it should also retain the flexibility to support bold, mission-aligned flagship projects that respond to Europe's most pressing digital challenges. These could include, for example: open cloud infrastructure components that help reduce reliance on hyperscalers; secure, interoperable identity protocols; open source AI model frameworks and toolchains that meet EU values and regulatory standards; and, open source components widely used as industry standards in key areas like climate tech, health systems, or secure communications. While not the most important criteria – strategic investments should be chosen carefully and sparingly – the fund should be structurally capable of responding to these opportunities when they align with sovereignty, security, innovation, and competitiveness priorities. Doing so positions the EU-STF not just as a repair tool for fragile infrastructure, but as an engine for digital transformation in line with the EU's digital policy ambitions.

Recommendation #6 – Make sure the vehicle actively involves the open source community at every step of its inception, development and deployment: The open source ecosystem functions on transparency, trust, and decentralised collaboration, all principles that must be mirrored in the fund's governance and design. Involving community stakeholders in everything from project selection to oversight mechanisms helps prevent tokenism and ensures that the fund reflects the needs and realities of the people maintaining Europe's digital infrastructure. As the study notes, co-ownership is essential to long-term legitimacy and building trust with the open source community. In other words, the fund must be shaped "with, not for" the community, particularly with respect to co-design of funding criteria, oversight mechanisms, and transparent communication practices.

Recommendation #7 – Create a central governance structure that preserves the essential characteristics and personality of the German STF: The value of the German STF lies in its agility, community credibility, and mission-driven posture. The EU-STF must institutionalise these traits within a more complex governance framework. Preservation of its core principles – low bureaucracy, transparent processes, community orientation – must be baked into the central architecture. The fund should not only invest in technical fixes, but also build institutional capacity, ecosystem resilience, and collaboration. This includes mapping software dependencies, convening actors, supporting community infrastructure, and offering training – all identified as core functions in Section IV.

Recommendation #8 – Ensure the EU-STF has a core of staff larger than the German STF to support the oversight of the fund and serve as its ambassadors where necessary: The EU-wide ambition demands at least, but possibly higher than, the staffing of the Sovereign Tech Agency's current team. This study recommends building a core staff who can engage with national stakeholders, communicate priorities, and ensure ongoing coordination and knowledge transfer. Again, this may be complicated with an EDIC structure as it is currently understood, but there is a lot of flexibility in terms of the design of the EDIC, and to a lesser extent other joint structures. Ensuring that there is a core staff who does not just represent the interests of Member States but who can be trusted advisors and interlocutors with the open source ecosystem is mission critical.

VII. Conclusion

To implement the critical and timely vision for an EU-STF, EU officials and Member State policymakers must act with urgency, recognising that fragmented, short-term, or purely national efforts will not be sufficient to address Europe's digital challenges. Now, compared to other times in recent political history, there is more cover to do this, it simply requires policymakers to understand the arguments that have been presented here and rise to the occasion. The EU-STF offers the chance to demonstrate that Europe is ready to lead – not only in regulating technology but in investing in the open digital infrastructure that helps us ensure the open source fundamentals at the heart of our shared digital future. By seizing this moment, Europe can shift from reactive crisis management to proactive stewardship of its digital infrastructure, setting a valuable global example of how public investment can act as a force multiplier for Europe while demonstrating leadership globally. It is the right thing to do.

Endnotes

1. Opensource.com, "What is open source?", n.d., accessed on 21 July 2025, https://opensource.com/resources/what-open-source#:~:text=Open%20source%20software%20is%20software,or%20%22application%22%E2%80%94works.

2. Note that we use the term EU-STF as a shorthand for an EU version of the German Sovereign Tech Fund/Sovereign Tech Agency. The shorthand EU-STF, rather than EU-STA, is used because we are focused on setting up a fund and not an agency, as there are complications under EU law in setting up an agency (though the funding could be part of an executive agency; for more on this, see Section V). Thus, EU-STF should be taken as a stand-in for the concept of scaling such funding to the EU level more broadly.

3. Katherine Druckman, "The Careful Consumption of Open Source Software", n.d., https://www.intel.com/content/www/us/en/developer/articles/guide/the-careful-consumption-of-open-source-software.html#:~:text=Similarly%2C%20a%202022%20Linux%20Foundation,up%20of%20open%20source%20components.

4. A maintainer is the person or team responsible for keeping an open source project functional: fixing bugs, reviewing contributions, updating documentation, and releasing new versions. With OSS, these maintainers are often volunteers or part-time contributors, even when the software is used by governments, global firms, and national infrastructure.

5. Jordyn Alger, "Open source software vulnerabilities found in 86% of codebases", Security Magazine, 25 February 2025, https://www.securitymagazine.com/articles/101420-open-source-software-vulnerabilities-found-in-86-of-codebases.

6. xkcd, "Dependency", n.d., https://xkcd.com/2347/.

7. Nadia Eghbal, "Roads and Bridges: The Unseen Labor Behind Our Digital Infrastructure", Ford Foundation, 14 July 2016,

8. This term is similarly used in the framing of investment in open source foundations by the German STF, which treats open source code and OSS as digital infrastructure, what they call 'open digital infrastructure'.

9. Open Source Observatory, "Status of Open Source Software Policies in Europe 2020", 2020, https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/OSOR_Status%20of%20OSS%20Policies%20in%20Europe_2020_0.pdf.

10. For more information on the journey of the EC-OSPO, see: Gijs Hillenius, "Free/open source at the European Commission, OSPO Alliance On Ramp at European Commission OSPO, 16 May 2025, https://ospo-alliance.org/resources/onramp/20250516_ospo_onramp_open_source_at_the_ec.pdf.

11. Stewart Scott et. al, "Avoiding the success trap: Towards policy for open-source software as infrastructure", Atlantic Council, 8 February 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/open-source-software-as-infrastructure/.

12. EuropeanUnion Aviation Safety Agency, "Statement of revenue and expenditure for the 2024 financial year – European Union Aviation Safety Agency (EASA) – amending budget No 1", Publications Office of the European Union, 31 January 2025, https://op.europa.eu/en/publication-detail/-/publication/837b70f5-df74-11ef-be2a-01aa75ed71a1/language-en.

13. EUROCONTROL, "EUROCONTROL Agency Annual Accounts: As at 31 December 2023", 13 August 2024, https://www.eurocontrol.int/sites/default/files/2024-08/eurocontrol-annual-accounts-2023.pdf.

14. See: European Commission Energy, Climate change, Environment, "Waste Framework Directive", accessed on 21 July 2025, https://environment.ec.europa.eu/topics/waste-and-recycling/waste-framework-directive_en.

15. See: "European Securities and Markets Authority", accessed on 21 July 2025, https://www.esma.europa.eu/.

16. See: "Connecting Europe Facility", accessed on 21 July 2025, https://transport.ec.europa.eu/transport-themes/infrastructure-and-investment/connecting-europe-facility_en.

17. The feasibility of this fund was previously established in a report on the feasibility of the original German STF. For more information, see: Open Knowledge Foundation Deutschland, "Feasibility Study to Examine a Funding Program for Open Digital Base Technologies as the Foundation for Innovation and Digital Sovereignty", Sovereign Tech Fund, October 2021, https://www.sovereign.tech/public/files/SovereignTechFund_FeasibilityStudy.pdf.

18. Ibid, p. 3 and p. 9.

19. See: "EuroStack", accessed on 21 July 2025, https://eurostack.eu/.

20. These aspects were prioritised based on the interviews completed for this study and will be elaborated in future sections.

21. https://www.frontiersin.org/journals/education/articles/10.3389/feduc.2024.1356629/full

22. See: "Fraunhofer ISI", accessed on 21 July 2025, https://www.isi.fraunhofer.de/.

23. See: "European University Institute", accessed on 21 July 2025, https://www.eui.eu/en/home.

24. See: "OpenForum Europe", accessed on 21 July 2025, https://openforumeurope.org/.

25. As a baseline assumption of this study has been, it has been presumed the sheer scale of the usage of open source is a clear fact, but that the exact dependencies are difficult to point to. This will be pointed to later as a point for further research, although the Census II and Census III lists from Alpha/Omega might provide a compelling starting point. More information can be found at: Frank Nagle et. al, "Census II of Free and Open Source Software — Application Libraries", The Linux Foundation, March 2022, https://www.linuxfoundation.org/hubfs/Research%20Reports/lfr_harvard_censusII_mar2022_042824b.pdf?hsLang=en; Frank Nagle et. al, "Census III of Free and Open Source Software: Application Libraries", The Linux Foundation December 2024, https://www.linuxfoundation.org/hubfs/LF%20Research/lfr_censusiii_120424a.pdf?hsLang=en.

26. The study is being released in July 2025 in order to provide direct insights that can contribute to the MFF. This study expands on a proposal we had already submitted as a response to the MFF consultation period's call for input, which proposed at a high level how the EU should fund the establishment of an EU-STF.

27. Luca Zorloni, "The EU Is Taking on Big Tech. It May Be Outmatched", Wired, 9 June 2024, https://www.wired.com/story/european-commission-big-tech-regulation-outlook/?.

28. Ralf Boscheck, "The EU's Digital Markets Act: Regulatory Reform, Relapse or Reversal?", Intereconomics: Review of European Economic Policy 59, no. 3 (2024), https://www.intereconomics.eu/contents/year/2024/number/3/article/the-eu-s-digital-markets-act-regulatory-reform-relapse-or-reversal.html?.

29. Klaudia Majcher, "Coherence between Data Protection and Competition Law in Digital Markets", Oxford Scholarship Online (2023), https://doi.org/10.1093/oso/9780198885610.001.0001.

30. Klaudia Majcher, "Interaction between EU competition law and data protection in digital markets: striving for coherence", in Research Handbook On Competition And Technology ed. Luigi Parcu, Maria Alessandra Rossi, and Marco Botta, Elgar Publishing (2025), https://www.elgaronline.com/edcollchap/book/9781035302642/chapter15.xml?.

31. While the concept is more discussed in recent months, this reflects the synthesis of EU digital policy priorities as articulated in the European Commission's Path to the Digital Decade (2023) and the European Council Conclusions on Digital Policy Priorities (2024), where digital sovereignty features as a guiding concept underpinning various initiatives. Conversations around digital sovereignty began much earlier than that even, particularly in Member States (for example, the German Council Presidency in 2020).

32. Ian Brown, "Towards European Digital Independence", Data protection and digital competition by Ian Brown, Douwe Korff and friends, 26 September 2024, https://www.ianbrown.tech/2024/09/26/2061/.

33. Thomas Claburn, "European pols wave their hands about digital sovereignty with broad but vague plan", The Register, 6 June 2025, https://www.theregister.com/2025/06/06/europe_international_digital_strategy_nothingburger/.

34. Irina Kolupaieva and Larysa Tiesheva, "Asymmetry and convergence in the development of digital technologies in the EU countries", Quarterly Journal of Economics and Economic Policy 18, no. 3 (2023), https://doi.org/10.24136/eq.2023.022.

35. See: Forbes, "Top 100 Digital Companies List", n.d., accessed on 21 July 2025, https://www.forbes.com/top-digital-companies/list/.

36. Maximilian Mayer and Yen-Chi Lu, "Global structures of digital dependence and the rise of technopoles", New Political Economy, 5 May 2025, https://doi.org/10.1080/13563467.2025.2497766.

37. EUR-Lex: Access to European Union law, "Decision (EU) 2022/2481 of the European Parliament and of the Council of 14

December 2022 establishing the Digital Decade Policy Programme 2030 (Text with EEA relevance)", European Union, n.d., https://eur-lex.europa.eu/eli/dec/2022/2481/oj.

38. European Parliament, "EU AI Act: first regulation on artificial intelligence", 8 June 2023,

39. See: European Commission, "Chips Act", accessed on 21 July 2024, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en.

40. See: European Commission Business, Economy, Euro, "The Digital Markets Act", European Commission, n.d., accessed on 21 July 2025, https://digital-markets-act.ec.europa.eu/index_en.

41. See: European Commission Shaping Europe's digital future, "The Digital Europe Programme", n.d., European Commission, accessed on 21 July 2025, https://digital-strategy.ec.europa.eu/en/activities/digital-programme.

42. See: European Commission Research and Innovation, "Horizon Europe", European Commission, n.d., accessed on 21 July 2025, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.

43. See: "Gaia-X", accessed on 21 July 2025, https://gaia-x.eu/.

44. See: European Commission EU Digital Identity Wallet, "A digital ID and

45. See: European Commission Shaping Europe's digital future, "2025 State of the Digital Decade package", European Commission, accessed on 21 July 2025, https://digital-strategy.ec.europa.eu/en/policies/2025-state-digital-decade-package.

46. In his landmark Sorbonne speech on 26 September 2017, President Macron placed digital technology squarely within Europe's sovereignty agenda – arguing that building an "innovative, sovereign Europe" required not just policy and regulation, but concrete investments in digital infrastructure and capabilities. See: Élysée, "President Macron gives speech on new initiative for Europe", 26 September 2017, https://www.elysee.fr/en/emmanuel-macron/2017/09/26/president-macron-gives-speech-on-new-initiative-for-europe?.

47. For example, in January 2024, President Macron and German Chancellor Olaf Scholz jointly wrote that Europe must "reduce our critical dependencies" and strengthen its sovereignty – calling for investment in strategic digital technologies such as AI, quantum, 5G/6G infrastructure, and public procurement of key digital capabilities. See: Olaf Scholz, "Macron and Scholz: we must strengthen European sovereignty", The Financial Times, 27 May 2024, https://www.ft.com/content/853f0ba0-c6f8-4dd4-a599-6fc5a142e879.

48. Commons Network, "French Digital Commons Proposal", n.d., accessed on 21 July 2025, https://www.commonsnetwork.org/12328-2/.

49. See: "ZenDis", accessed on 21 July 2025, https://www.zendis.de/.

50. Sean Endicott, "It's the year of Linux... at least for Denmark — here's why the country's government is dumping Windows and Office 365", Windows Central, 14 June 2025,

51. OpenForum Europe, "Open Strategic Autonomy: Ensuring Europe's Access to Key Enabling Technologies, Reducing Dependencies and Growing Capabilities", March 2022, https://openforumeurope.org/wp-content/uploads/2022/03/Open-Strategic-Autonomy-OFE-March-2022.pdf.

52. See: European Commission Shaping Europe's Digital Future, "NIS2 Directive: securing network and information systems", European Commission, accessed on 21 July 2025, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

53. See: European Commission Shaping Europe's Digital Future, "EU Cybersecurity Act", accessed on 21 July 2025, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

54. Marc Schuler and Julie Dumontet, "Cyber security and open-source software in products with digital elements", TaylorWessing, 24 March 2025, https://www.taylorwessing.com/de/global-data-hub/2025/digital-resilience-and-cyber-security/gdh---cyber-security-and-open-source-software-in-products-with-digital-elements#:~:text=The%20Cyber%20Resilience%20Act%20(CRA,the%20obligations%20of%20the%20CRA.

55. Mirko Swillus, "What open source maintainers shared with us", Sovereign Tech Agency, 9 October 2024, https://

www.sovereign.tech/news/what-open-source-maintainers-shared-with-us&sa=D&source=docs&ust=1752233167460787&usg=AOvVaw1z9a0-5z_pYhc_uVuFRTFc.

56. European Union Agency for Cybersecurity. "Foresight Cybersecurity Threats for 2030 – Update", March 2024, https://www.enisa.europa.eu/sites/default/files/2024-11/Cybersecurity%20Threats%20for%202030%20-%20Update%202024%20-%20Executive%20Summary_0.pdf.

57. Nikolay Harutyunyan, "Managing Your Open Source Supply Chain-Why and How?", Computer 53, no. 6 (2020): 77–81, https://www.doi.org/10.1109/MC.2020.2983530.

58. Manuel Hoffmann et. al, "The Value of Open Source Software", SSRN Journal, Harvard Business School Strategy Unit Working Paper no. 24-038 (2024). http://dx.doi.org/10.2139/ssrn.4693148.

59. Ibid.

60. European Union Agency for Cybersecurity. "Foresight Cybersecurity Threats for 2030 – Update", p. 12.

61. Akamai Security Intelligence Group, "XZ Utils Backdoor — Everything You Need to Know, and What You Can Do", Akamai, 1 April 2024, https://www.akamai.com/blog/security-research/critical-linux-backdoor-xz-utils-discovered-what-to-know.

62. Robert Sheldon, "What is Unix?", TechTarget, 9 February 2025, https://unix.org/.

63. Andy Greenberg and Matt Burgess, "The Mystery of 'Jia Tan,' the XZ Backdoor Mastermind", Wired, 3 April 2024, https://www.wired.com/story/jia-tan-xz-backdoor/.

64. Piergiorgio Ladisa et. al, "Taxonomy of Attacks on Open-Source Software Supply Chains", IEEE Symposium on Security and Privacy (SP) (2023): 1509-1526, https://doi.org/10.48550/arXiv.2204.04008.

65. Marc Ohm et. al, "Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks", in Detection of Intrusions and Malware, and Vulnerability Assessment, 17th International Conference ed. Clémentine Maurice, Leyla Bilge, Gianluca Stringhini and Nuno Neves (2020): 22-43, https://doi.org/10.1007/978-3-030-52683-2_2.

66. Venu Shastri, "What is a Zero-Day Exploit?", CrowdStrike, 17 January 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/zero-day-exploit/.

67. For more on malicious backdoors, see again the XZ utils case: C2A Security, "Dangerous Backdoor Found in Two XZ Utils Versions – Implications and Risk", 5 April 2024, https://c2a-sec.com/dangerous-backdoor-found-in-two-xz-utils-versions-implications-and-risk/#:~:text=This%20vulnerability%20was%20introduced%20into%20an%20open%2Dsource,and%20potential%20control%20of%20the%20entire%20machine.

68. Xuetao Li et. al, "Systematic Literature Review of Commercial Participation in Open Source Software", in ACM Transactions on Software Engineering and Methodology 34, no. 2, art. 33 (2025): 1–31, https://doi.org/10.1145/3690632.

69. Cailean Osborne, "Public-private funding models in open source software development: A case study on scikit-learn", arXiv, 3 May 2024, https://doi.org/10.48550/arXiv.2404.06484.

70. Mathieu O'Neil et. al, "Co-producing industrial public goods on GitHub: Selective firm cooperation, volunteer-employee labour and participation inequality", in New Media and Society 26, no. 5 (2024): 2556-2592, https://doi.org/10.1177/14614448221090474.

71. Jinfang Niu, "Addressing the free-rider problem in collectively built online archives", in Archives and Museum Informatics 25, no. 2 (2025), https://doi.org/10.1007/s10502-025-09480-2.

72. Adrienn Lawson and Stephen Hendrick, "Unaware and Uncertain: The Stark Realities of Cyber Resilience Act Readiness in Open Source", The Linux Foundation, March 2025, https://www.linuxfoundation.org/hubfs/Research%20Reports/lfr_cra_readiness_050125a.pdf?hsLang=en&utm.

73. Center for Strategic & International Policies, "Government Open Source Software Policies", n.d., accessed on 21 July 2025, https://www.csis.org/programs/strategic-technologies-program/resources/government-open-source-software-policies.

74. China has embraced OSS as a strategic pillar of its digital infrastructure, presenting open source as an "industrial policy tool" that bolsters technological autonomy and domestic innovation. See: Rebecca Arcesati and Caroline Meinhardt, "MERICS Primer –

China's Open-Source Tech Development: Insights into a growing ecosystem", MERICS, May 2021, p.3, https://merics.org/sites/default/files/2021-05/MERICS%20Primer%20Open%20Source%202021_0.pdf?.

75. South Korea has embedded OSS into its public sector architecture: its 2014 OSS Invigoration Plan and the amended 2020 Software Promotion Act mandate open source disclosure in government-funded software, reduce vendor lock-in, and foster open standards across e-government platforms. See: Open Source Observatory, "OSS Country Intelligence Factsheet – Open Source Policy: South Korea", European Commission, August 2021, https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/OSS%20Country%20intelligence%20factsheet_KR.pdf?.

76. Johan Linåker et. al, "Open Source Software in the Public Sector: 25 years and still in its infancy", IEEE Computer Society, 2019, p.2, http://dx.doi.org/10.1109/MS.2023.3266105.

77. Rachel Layne, "Open Source Software: The $9 Trillion Resource Companies Take for Granted", Working Knowledge at Harvard Business School (blog), 22 March 2024, https://www.library.hbs.edu/working-knowledge/open-source-software-the-nine-trillion-resource-companies-take-for-granted.

78. Knut Blind et. al, "Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy", European Commission, 2 September 2021, https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and.

79. VDA (press release), "Automotive industry signs Memorandum of Understanding for joint software development based on open source", 24 June 2025, https://www.vda.de/en/press/press-releases/2025/250624_PM_Automotive_industry_signs_Memorandum_of_Understanding.

80. Manuel Hoffmann et. al, "The Value of Open Source Software".

81. Knut Blind and Torben Schubert, "Estimating the GDP effect of Open Source Software and its complementarities with R&D and patents: evidence and policy implications", in Journal of Technology Transfer 49, no. 2 (2024): 466–491, https://doi.org/10.1007/s10961-023-09993-x.

82. European Commission Shaping Europe's digital future, "Commission publishes study on the impact of Open Source on the European economy", European Commission, 6 September 2021, https://digital-strategy.ec.europa.eu/en/news/commission-publishes-study-impact-open-source-european-economy.

83. Alasdair Young, "Governing the digital economy: transatlantic accommodation and cooperation", in Journal of European Integration 46, no. 7 (2024): 973–992, https://doi.org/10.1080/07036337.2024.2398429.

84. Ioanna Hadjiyianni, "The European Union as a Global Regulatory Power". in Oxford Journal of Legal Studies 41, no. 1 (2021): 243–264, https://doi.org/10.1093/ojls/gqaa042.

85. Alasdair Young, "Governing the digital economy: transatlantic accommodation and cooperation".

86. Anu Bradford, "Digital empires. The global battle to regulate technology", Oxford University Press, September 2023, https://doi.org/10.1093/oso/9780197649268.001.0001.

87. Mario Draghi, "The Draghi report on EU competitiveness", European Commission, 9 September 2024, https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en.

88. Red Hat, "The power of open source: why it underpins digital transformation", 22 September 2020, https://www.cio.com/article/194038/the-power-of-open-source-why-it-underpins-digital-transformation.html.

89. Eleonora Francica, Martin Greenacre and Goda Naujokaitytė, "Commission draft proposal for FP10 leaked", Science|Business, 8 July 2025, https://sciencebusiness.net/news/planning-fp10/commission-draft-proposal-fp10-leaked.

90. Muhammed Furkan Akıncı, Legal Challenges and Opportunities in Regulation Free and Open Source Software within the European Union", in The Boğaziçi Law Review 2, no. 1 (2024): 1-20, https://doi.org/10.69800/blr.1467329.

91. Andreas Liesenfeld and Mark Dingemanse, "Rethinking open source generative AI: open washing and the EU AI Act", in FAccT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency (2024): 1774–1787, https://doi.org/

10.1145/3630106.3659005.

92. McKinsey & Company, "Open source technology in the age of AI", QuantumBlack AI by McKinsey, 22 April 2025, https://www.mckinsey.com/capabilities/quantumblack/our-insights/open-source-technology-in-the-age-of-ai.

93. Filippo Gualtiero Blancato, "The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem", in Policy & Internet 16, no. 1 (2024), 12–32, https://doi.org/10.1002/poi3.358.

94. Daria Golebiowska-Tataj, "Enhancing European Competitiveness with Fairness, Sustainability and Open Strategic Autonomy", European Commission JRC Publications Repository, JRC Working Paper Series For a Fair, Innovative and Sustainable Economy no. 14 (2024): 1-13, https://publications.jrc.ec.europa.eu/repository/handle/JRC139560.

95. Vineet, Kumar, Brett R. Gordon and Kannan Srinivasan, "Competitive Strategy for Open Source Software", in Marketing Science 30, no. 6 (2011): 1066-1078, https://doi.org/10.1287/mksc.1110.0669.

96. Eelko K.R.E. Huizingh, "Open innovation: State of the art and future perspectives", in Technovation 31, no. 1 (2011): 2–9, https://doi.org/10.1016/j.technovation.2010.10.002.

97. Henry Chesbrough, "Open Innovation: A New Paradigm for Understanding Industrial Innovation", in Henry Chesbrough (Hg.): Open innovation. Researching a new paradigm, Oxford University Press (2006): 1-12, https://doi.org/10.1093/oso/9780199290727.001.0001.

98. Knut Blind et. al, "Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy".

99. Justin Pappas Johnson, "Open Source Software: Private Provision of a Public Good", in Journal of Economics & Management Strategy 11, no. 4 (2002): 637–662, https://doi.org/10.1111/j.1430-9134.2002.00637.x.

100. Inge Kaul, "Global public goods", in The International Library of Critical Writings in Economics Series ed. Inge Kaul, Edward Elgar Publishing (2016), https://www.e-elgar.com/shop/gbp/global-public-goods-9781783472994.html.

101. Dries Buytaert, "Open source and the free-rider problem", InfoWorld, 6 November 2019, https://www.infoworld.com/article/2264054/open-source-and-the-free-rider-problem.html.

102. Nadia Eghbal, "Working in Public: The Making and Maintenance of Open Source Software", Stripe Press, August 2020, p. 155-168, https://press.stripe.com/working-in-public.

103. Eric von Hippel, "Democratizing Innovation", MIT Press, February 2005, https://doi.org/10.7551/mitpress/2333.001.0001.

104. Chinmayi Sharma, "Tragedy of the Digital Commons", North Carolina Law Review (2023): 1129-1228, http://dx.doi.org/10.2139/ssrn.4245266.

105. Nadia Eghbal, "Working in Public: The Making and Maintenance of Open Source Software", p. 155-168.

106. As Eghbal points out, a handful of maintainers often are responsible for the majority of contributions and maintenance work. See: Nadia Eghbal, "Working in Public: The Making and Maintenance of Open Source Software", p. 155-168.

107. This systemic approach is crucial because the attention depletion problem requires ecosystem-wide solutions rather than piecemeal interventions, especially when you consider the needs of ODBTs, which attract fewer contributors – and therefore resources – in the first place.

108. Boysel et. al, "2024 Open Source Software Funding Report", The Linux Foundation, 19 November 2024, https://opensourcefundingsurvey2024.com.

109. Open source foundations are different in this regard, but also do not solve the whole problem. They occupy a middle ground by focusing on governance, maintainer support, and ecosystem-wide coordination rather than feature development, making them more effective than traditional private funding at addressing attention scarcity. However, foundations still face resource constraints, corporate influence, and selective coverage that limits their ability to address systemic sustainability challenges across the entire open source ecosystem, suggesting continued need for broader public intervention.

110. Boysel et. al, "2024 Open Source Software Funding Report".

111. Nadia Eghbal, "Working in Public: The Making and Maintenance of Open Source Software", p. 191-208.

112. David A. Wheeler, "Insights into Open Source Software Usage and Security", DEVOPSdigest, 11 March 2025, https://www.devopsdigest.com/openssf-census-iii-report-2024.

113. Alexandros Tsakpinis and Alexander Pretschner, "Analyzing the Usage of Donation Platforms for PyPI Libraries", arXiv (2025): 1-6, https://doi.org/10.48550/arXiv.2503.08263.

114. Mariana Mazzucato, "The Entrepreneurial State: Debunking public vs. private sector myths", Anthem Press, https://marianamazzucato.com/books/the-entrepreneurial-state.

115. Ibid.

116. Knut Blind et. al, "Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy".

117. Cassandra Sweet and Dalibor Eterovic, "Do patent rights matter? 40 years of innovation, complexity and productivity", in Journal of World Development 115 (2019): 78–93, https://doi.org/10.1016/j.worlddev.2018.10.009.

118. Knut Blind, "Standardization and Standards: Safeguards of Technological Sovereignty?", in Technological Forecasting and Social Change 210 (2025), https://doi.org/10.1016/j.techfore.2024.123873.

119. Knut Blind et. al, "Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy".

120. Joshua Lerner and Mark Schankerman, "The comingled code. Open source and economic development", MIT Press, https://doi.org/10.7551/mitpress/9780262014632.001.0001.

121. Nataliya Langburd Wright, Frank Nagle and Shane Greenstein, "Open source software and global entrepreneurship", Journal of Research Policy 52, no. 9 (2023): 1-20, https://doi.org/10.1016/j.respol.2023.104846.

122. Justin Pappas Johnson, "Open Source Software: Private Provision of a Public Good".

123. Linus Dahlander and David M. Gann, "How open is innovation?", in Journal of Research Policy 39, no. 6 (2010): 699–709, https://doi.org/10.1016/j.respol.2010.01.013.

124. Knut Blind et. al, "Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy".

125. Brian Fitzgerald, Audris Mockus, Minghui Zhou, "Towards Engineering Free/Libre Open Source Software (FLOSS) Ecosystems for Impact and Sustainability", Springer, Communications of NII Shonan Meetings 1st ed. (2019): 1-13, https://dl.acm.org/doi/10.1145/3597503.3639230.

126. See: "The Linux Foundation", accessed on 21 July 2025, https://www.linuxfoundation.org/.

127. See: "The Apache Foundation", accessed on 21 July 2025, https://www.apache.org/.

128. See: "Eclipse Foundation", accessed on 21 July 2025, https://www.eclipse.org/.

129. Javier Luis Cánovas Izquierdo and Jordi Cabot, "The role of foundations in open source projects", in Valerie Issarny (Hg.): Proceedings of the 40th International Conference on Software Engineering Software Engineering in Society, Association for Computing Machinery-Digital Library (2018): 3–12, http://dx.doi.org/10.1145/3183428.3183438.

130. Morten Andersen-Gott, Gheorgita Ghinea and Bendik Bygstad, "Why do commercial companies contribute to open source software?", in International Journal of Information Management 32, no. 2 (2012): 106–117, https://doi.org/10.1016/j.ijinfomgt.2011.10.003.

131. Boysel et. al, "2024 Open Source Software Funding Report".

132. Mariana Mazzucato, "The Entrepreneurial State: Debunking public vs. private sector myths".

133. Science Europe, "Our priorities: EU Framework Programmes", n.d., accessed on 21 July 2025, https://scienceeurope.org/our-priorities/eu-framework-programmes/.

134. European Commission, "Competitiveness compass", n.d., accessed on 21 July 2025, https://commission.europa.eu/topics/eu-competitiveness/competitiveness-compass_en.

135. Johannes Lindner, Jannik Jansen and Thu Nguyen, "The German coalition agreement: What's in it for Europe?", Hertie School

Jacques Delors Centre, 17 April 2025, https://www.delorscentre.eu/en/publications/detail/publication/the-german-coalition-agreement-whats-in-it-for-europe.

136. Peter Strempel, "European autonomy in technology is about freedom to operate through strategic ownership, collaboration, and access", EIT Digital, 10 February 2021, https://www.eitdigital.eu/newsroom/news/2021/european-autonomy-in-technology-is-about-freedom-to-operate-through-strategic-ownership-collaboration-and-access/.

137. Understanding derived from: Pacific Northwest, "Cyber Resilience", n.d., accessed on 21 July 2025, https://www.pnnl.gov/explainer-articles/cyber-resilience.

138. See: "Next Generation Internet", accessed on 21 July 2025, https://www.ngi.eu/.

139. Clémentine Valayer, "Benchmarking the impact of the next generation internet initiative Final study report", Publications Office of the European Union, April 2024, https://op.europa.eu/en/publication-detail/-/publication/257ae66f-23c7-11ef-a195-01aa75ed71a1/language-en.

140. Osborne et. al, "A Toolkit for Measuring the Impacts of Public Funding on Open Source Software Development", arXiv, 2 November 2024, p. 6, http://dx.doi.org/10.48550/arXiv.2411.06027.

141. The NGI initiative is funded under the Horizon Europe framework programme for research and innovation. NGI functions as a key pillar of Horizon Europe's digital agenda, supporting research, experimentation, and deployment of open, human-centric internet technologies, often through cascade funding mechanisms to SMEs, researchers, and open source communities.

142. European Commission, "Cascade Funding Calls / Financial Support for Third Parties (FSTP)", EU Funding & Tenders Portal, n.d., accessed on 21 July 2025, https://webgate.ec.europa.eu/funding-tenders-opportunities/pages/viewpage.action?pageId=25559615.

143. Eleonora Francica, Martin Greenacre and Goda Naujokaitytė, "Commission draft proposal for FP10 leaked".

144. European Commission, "European Commission's Open Source Programme Office starts bug bounties", 19 January 2022, https://commission.europa.eu/news-and-media/news/european-commissions-open-source-programme-office-starts-bug-bounties-2022-01-19_en.

145. For example, see: European Commission, "EU-FOSSA 2 - the EU's open source cybersecurity project ends", 14 July 2020, https://commission.europa.eu/news-and-media/news/eu-fossa-2-eus-open-source-cybersecurity-project-ends-2020-07-14_en.

146. Osborne et. al, "A Toolkit for Measuring the Impacts of Public Funding on Open Source Software Development", p 4.

147. JEDI | The European ARPA, "About", n.d., accessed on 21 July 2025, https://www.jedi.foundation/about.

148. Ibid.

149. European Commission Shaping Europe's Digital Future, "European Digital Infrastructure Consortium - EDIC", European Commission, n.d., accessed on 21 July 2025, https://digital-strategy.ec.europa.eu/en/policies/edic.

150. NL Digital Government, "European Collaboration for Digital Commons", 18 July 2024, https://www.nldigitalgovernment.nl/news/european-collaboration-for-digital-commons/.

151. See: "Open Technology Fund", accessed on 21 July 2025, https://www.opentech.fund/.

152. Technology Modernization Fund, "Our process", n.d., accessed on 21 July 2025, https://tmf.cio.gov/process/.

153. Human Rights Watch, "US: Fight Continues for Open Technology Fund's Independence", 20 August 2020, https://www.hrw.org/news/2020/08/20/us-fight-continues-open-technology-funds-independence.

154. See: "Open Source Technology Improvement Fund", accessed on 21 July 2025, https://ostif.org/.

155. Open Source Technology Improvement Fund, "About", n.d., accessed on 21 July 2025, https://ostif.org/about/.

156. Sourced from conversations directly with the OSTIF team.

157. Sovereign Tech Agency, "Sovereign Tech Fund", n.d., accessed on 21 July 2025, https://www.sovereign.tech/programs/fund.

158. In 2023, about EUR €11.5 million was allocated, rising to roughly EUR €17 million in 2024 and EUR €20 million in 2025; though the latter remains pending due to Germany's interim budget following snap elections.

159. Sovereign Tech Fund, "Evaluation Report Pilot Phase", April 2023, https://www.sovereign.tech/public/files/SovereignTechFund_Evaluation_Report_Pilot_Phase.pdf.

160. See: "SerNet", accessed on 21 July 2025, https://www.sernet.com/.

161. Liam Proven, "Germany's Sovereign Tech Fund throws cash at FreeBSD and Samba", The Register, 1 October 2024, https://www.theregister.com/2024/10/01/freebsd_and_samba_funding/.

162. See: "FreeBSD", accessed on 21 July 2025, https://www.freebsd.org/.

163. Note: The German STF does not explicitly classify projects in this way.

164. See: "OpenBLAS", accessed on 21 July 2025, https://www.openblas.net/.

165. "OpenJS Foundation", accessed on 21 July 2025, https://openjsf.org/.

166. See: "FFmpeg", accessed on 21 July 2025, https://ffmpeg.org/.

167. "The Yocto Project", accessed on 21 July 2025, https://www.yoctoproject.org/.

168. "GNOME", https://www.gnome.org/.

169. Powen Shiah, "Celebrating two years of empowering public digital infrastructure", Sovereign Tech Agency, 18 October 2024, https://www.sovereign.tech/news/celebrating-two-years-of-empowering-public-digital-infrastructure.

170. European Commission Shaping Europe's Digital Future, "Digital Europe Programme: €7.5 billion of funding for 2021-2027", European Commission (factsheet), 4 June 2020, https://digital-strategy.ec.europa.eu/en/library/digital-europe-programme-eu75-billion-funding-2021-2027.

171. European Commission Research and innovation, "How Horizon Europe was developed", European Commission, n.d., accessed on 21 July 2025, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/how-horizon-europe-was-developed_en.

172. European Commission, "European Chips Act", n.d., accessed on 21 July 2025, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en.

173. The Sovereign Tech Fund has partnered with the OSTIF, for its Sovereign Tech Resilience Program. For more information, see: Open Source Technology Improvement Fund and Sovereign Tech Agency, "2024 Sovereign Tech Agency Security Audit Impact Report", OSTIF, 2024, https://ostif.org/wp-content/uploads/2025/01/2024-Sovereign-Tech-Agency_OSTIF-Impact-Report.pdf.

174. Note: This would not mean erasing the work being done by CRA expert groups. For more information, see: European Commission Shaping Europe's digital future, "Cyber Resilience Act", European Commission, n.d., accessed on 21 July 2025, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

175. Importantly, this effort can leverage mechanisms introduced under the CRA: manufacturers of products with digital elements will be required to submit Software Bills of Materials (SBOMs) to national market surveillance authorities, who will provide aggregated dependency information to the CRA Administrative Cooperation Group (ADCO) for EU-wide analysis (Art. 13(25) CRA).

176. Open Source Technology Improvement Fund, "Get an Audit", n.d., accessed on 21 July 2025, https://ostif.org/get-an-audit/.

177. OpenSSF, "Case Study: OSTIF Improves Security Posture of Critical Open Source Projects Through OpenSSF Membership", 13 July 2024, https://openssf.org/blog/2025/06/13/case-study-ostif-improves-security-posture-of-critical-open-source-projects-through-openssf-membership/.

178. OpenSSF, "Beyond the OpenSSF: An Introduction to Other Security Efforts Across the Linux Foundation", 30 May 2024, https://openssf.org/blog/2024/05/30/beyond-the-openssf-an-introduction-to-other-security-efforts-across-the-linux-foundation/.

179. Eclipse Foundation, "Security", n.d., accessed on 21 July 2025, https://www.eclipse.org/security/.

180. One example of an improvement project is the OpenJS Foundation Project which received funding from the German STF. The project was about implementing improvements to the JavaScript ecosystem infrastructure and security. JavaScript is the most widely used programming language and has helped transform the web from static to interactive and dynamic applications. Because of JavaScript's universal design and usefulness, projects that would be positively affected by this work can be found across sectors, fields, and regions. For more information, see: "OpenJS Foundation", accessed on 21 July 2025, https://openjsf.org/.

181. Note: The German STF operates within German public procurement rules but does so in a way that reduces the administrative burden on projects and directly contracts them, and something similar would need to be attempted at the EU level.

182. This must be both geographically and in terms of eligibility for individuals, independent contractors, non-profits, open source companies, and even employees whose work on open source projects could be subsidised through their employers.

183. Under Article 17(1) TEU, the EC has responsibility for implementing EU matters – and may decide which DG is responsible for what activities. Once delegated, DGs are responsible for both policy and implementation.

184. European Health and Digital Executive Agency, "Connecting Europe Facility: Digital", European Commission, n.d., accessed on 21 July 2025, https://hadea.ec.europa.eu/programmes/connecting-europe-facility_en.

185. European Commission Shaping Europe's digital future, "The Digital Europe Programme", European Commission, n.d., accessed on 21 July 2025, https://digital-strategy.ec.europa.eu/en/activities/digital-programme.

186. European Cybersecurity Competence Centre and Network, "The European Cybersecurity Competence Centre and Network", n.d., accessed on 21 July 2025, https://cybersecurity-centre.europa.eu/index_en.

187. European Health and Digital Executive Agency, "European Health and Digital Executive Agency", n.d., accessed on 21 July 2025, https://hadea.ec.europa.eu/index_en.

188. EUR-Lex, "COMMISSION STAFF WORKING DOCUMENT: Progress report on multi-country projects", European Commission, 16 June 2025, p. 3-6, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025SC0292#:~:text=The%20Communication%20on%20the%20Cybersecurity,%2C%20Austria%2C%20Croatia%20and%20Slovenia.

189. Ibid, p. 3. For a comprehensive list, the other characteristics mentioned by the EC are: (1) "help reduce the digital divide between Member States;" (2) "support an interconnected, interoperable and secure Digital Single Market;"and (3) "implement flagship initiatives for which cooperation among Member States is important."

190. European Commission, "Infringement procedure", n.d., accessed on 21 July 2025, https://commission.europa.eu/law/application-eu-law/implementing-eu-law/infringement-procedure_en.

191. European Commission Employment, Social Affairs and Inclusion, "European Pillar of Social Rights", European Commission, n.d., accessed on 21 July 2025, https://employment-social-affairs.ec.europa.eu/policies-and-activities/european-pillar-social-rights-building-fairer-and-more-inclusive-european-union_en.

192. Beatrice Bertarini, "Chapter 2: Affirmation of the Digital Single Market and Related Regulatory Frameworks", in European Union Digital Single Market: Legal Framework and Challenges, FrancoAngeli (2023), https://hdl.handle.net/10419/279839.

193. See: "SPRIN-D", accessed on 21 July 2025, https://www.sprind.org/en.

194. European Innovation Council and SMEs Executive Agency, "EISMEA", European Commission, n.d., 21 July 2025, https://eismea.ec.europa.eu/index_en.

195. European Climate, Infrastructure and Environment Executive Agency, "CINEA", European Commission, n.d., 21 July 2025, https://cinea.ec.europa.eu/index_en.

196. European Health and Digital Executive Agency, "Operational Digital Platforms", European Commission, n.d., accessed on 21 July 2025, https://hadea.ec.europa.eu/programmes/connecting-europe-facility/about/operational-digital-platforms_en#:~:text=ODPs%20are%20physical%20and%20virtual,transport%20and%2For%20energy%20data.

197. European Commission, "Lump sum funding in Horizon Europe", EU Funding & Tenders Portal, n.d., accessed on 21 July 2025, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/horizon/lump-sum/opportunities.

198. VPH Institute, "European Commission Establishes HaDEA", n.d., accessed on 21 July 2025, https://www.vph-institute.org/news/european-commission-establishes-hadea.html.

199. European Health and Digital Executive Agency, "HERA Info Day", European Commission, n.d., accessed on 21 July 2025, https://hadea.ec.europa.eu/events/hera-info-day-2025-05-13_en.

200. EUR-Lex, "Commission Decision (EU) 2024/3082 of 4 December 2024 on transparency measures concerning meetings held

between Commission staff holding management functions and interest representatives, and repealing Decision 2014/838/EU, Euratom", European Commission, n.d., accessed on 21 July 2025, https://eur-lex.europa.eu/eli/dec/2024/3082/oj/eng.

201. EUR-Lex, "Council Regulation (EC) No 58/2003 of 19 December 2002 laying down the statute for executive agencies to be entrusted with certain tasks in the management of Community programmes", European Commission, n.d., accessed on 21 July 2025, https://eur-lex.europa.eu/eli/reg/2003/58/oj/eng.

202. Ibid, Art. 3.

203. Ibid, Art. 4.

204. Ibid, Art. 7.

205. See, in particular: ECJ, Case 9/56, Meroni v High Authority (1958) and Case 98/80, Romano (1981).

206. EUR-Lex, "Glossary of summaries: Joint Undertakings", European Commission, n.d., accessed on 21 July 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:joint_undertaking.

207. EUR-Lex, "Consolidated Version of the Treaty on the Functioning of the European Union", European Union, 26 October 2012, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF.

208. EUR-Lex, "Council Regulation (EU) 2021/2085 of 19 November 2021 establishing the Joint Undertakings under Horizon Europe and repealing Regulations (EC) No 219/2007, (EU) No 557/2014, (EU) No 558/2014, (EU) No 559/2014, (EU) No 560/2014, (EU) No 561/2014 and (EU) No 642/2014", European Union, n.d., accessed on 21 July 2025, https://eur-lex.europa.eu/eli/reg/2021/2085/oj/eng.

209. These included: Single European Sky ATM Research (SESAR), Electronic Components and Systems for European Leadership (ECSEL), IMI2, Clean Sky 2, FCH2, Shift2Rail, and Bio-Based Industries (BBI) JUs.

210. These include the European Smart Networks and Services (SNS) JU and the Global Health European & Developing Countries Clinical Trials Partnership (EDCTP3) JU.

211. European Union, "EU Joint Undertaking: Chips Joint Undertaking", n.d., accessed on 21 July 2025, https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/chips-joint-undertaking_en?.

212. Chips JU, "Chips for Europe Initiative", n.d., accessed on 21 July 2025, https://www.chips-ju.europa.eu/Pilot-lines/.

213. European Documentation Center (EDC) of the University of Almeria, "Commission launches Chips Joint Undertaking under the European Chips Act", n.d., accessed on 21 July 2025, https://www.cde.ual.es/en/commission-launches-chips-joint-undertaking-under-the-european-chips-act/.

214. EUR-Lex, "Council Regulation (EU) 2018/1488 of 28 September 2018 establishing the European High Performance Computing Joint Undertaking", European Union, n.d., accessed on 21 June 2025, https://eur-lex.europa.eu/eli/reg/2018/1488/oj/eng.

215. Under the Council Regulation (EU) 2021/1173 and and recently amended by Council Regulation (EU) 2024/1732. See: EUR-Lex, "Council Regulation (EU) 2024/1732 of 17 June 2024 amending Regulation (EU) 2021/1173 as regards a EuroHPC initiative for start-ups in order to boost European leadership in trustworthy artificial intelligence", European Union, n.d., accessed on 21 July 2025, https://eur-lex.europa.eu/eli/reg/2024/1732/oj/eng.

216. LUMI, "About LUMI", n.d., accessed on 21 July 2025, https://www.lumi-supercomputer.eu/about-lumi/.

217. EuroHPC Joint Undertaking, "Consolidated Annual Activity Report 2023 – The European High Performance Joint Undertaking", Annex to the EuroHPC Governing Board Decision no. 27, 28 June 2024, https://eurohpc-ju.europa.eu/document/download/5a49dad1-75fe-459c-9923-23b732e4b3a5_en?filename=Annex%20to%20EuroHPC%20JU%20Decision%20No%2027.2024%20-%20Consolidated%20Annual%20Activity%20Report%202023.pdf.

218. European Commission, "What is an EDIC?", 11 September 2023, https://ec.europa.eu/newsroom/lds/items/797960/en.

219. Ibid.

220. EUR-Lex, "Commission Implementing Decision (EU) 2024/458 of 1 February 2024 on setting up the European Digital Infrastructure Consortium for the Alliance for Language Technologies (ALT-EDIC)", European Union, n.d., accessed on 21 July 2025,

https://eur-lex.europa.eu/eli/dec_impl/2024/458/oj.

221. EUR-Lex, "Commission Implementing Decision (EU) 2024/1432 of 21 May 2024 setting up the European Digital Infrastructure Consortium for European Blockchain Partnership and European Blockchain Service Infrastructure (EUROPEUM-EDIC)", European Union, n.d., accessed on 21 July 2025, https://eur-lex.europa.eu/eli/dec_impl/2024/1432/oj/eng.

222. EUR-Lex, "Commission Implementing Decision (EU) 2024/459 of 1 February 2024 on setting up the European Digital Infrastructure Consortium for Networked Local Digital Twins towards the CitiVERSE (LDT CitiVERSE EDIC)", European Union, n.d., accessed on 21 July 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024D0459&qid=1748336997264.

223. EUR-Lex, "COMMISSION STAFF WORKING DOCUMENT: Progress report on multi-country projects".

224. European Commission, "What are the main features of an EDIC?", 11 September 2023, https://ec.europa.eu/newsroom/lds/items/798916/en.

225. EUR-Lex, "Commission Implementing Decision (EU) 2024/458 of 1 February 2024 on setting up the European Digital Infrastructure Consortium for the Alliance for Language Technologies (ALT-EDIC)", Annex II.

226. EUR-Lex, "Commission Implementing Decision (EU) 2024/1432 of 21 May 2024 setting up the European Digital Infrastructure Consortium for European Blockchain Partnership and European Blockchain Service Infrastructure (EUROPEUM-EDIC)", Annex III.

227. NL Digital Government, "Application for EDIC Digital Commons Submitted", 11 July 2025, https://www.nldigitalgovernment.nl/news/application-for-edic-digital-commons-submitted/.

228. NL Digital Government, "European Collaboration for Digital Commons".

229. N.A., "Digital Commons European Digital Infrastructure Consortium – DC-EDIC", Opensourcewerken, n.d., accessed on 21 July 2025, https://opensourcewerken.nl/attachment/entity/ac99644d-ca8b-4e71-9a07-33b22d3fa6c4.

230. EUR-Lex, "COMMISSION STAFF WORKING DOCUMENT: Progress report on multi-country projects", p. 9-10.

231. The first EDICs are in the very early stages of their setup, and the one with the closest precedent – the Digital Commons EDIC – is still awaiting official approval and has had its own complications.

232. NL Digital Government, "Application for EDIC Digital Commons Submitted".

233. It is worth noting that EC has a veto on the decisions of the Assembly of Members in certain circumstances, but that is more of a restriction than an enabling factor for coordination.

234. EUR-Lex, "Consolidated Version of the Treaty on the Functioning of the European Union".

235. European Commission Directorate-General for Competition, "Participating in an Important Project of common European Interest: Technical guidance on conditions and process", European Commission, n.d., accessed on 21 July 2025, https://competition-policy.ec.europa.eu/document/download/279cbfaf-49b1-4b90-b8f7-89d1f4a21eb3_en?filename=JEF_IPCEI_technical-guidance-calls.pdf&prefLang=lv.

236. As defined by EU case law. See: EUR-Lex: "Judgment of the Court (Sixth Chamber) of 23 April 1991. Klaus Höfner and Fritz Elser v Macrotron GmbH.", European Commission, n.d., accessed on 21 July 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:61990CJ0041.

237. That said, there is no binding requirement on the number of member states needed for setting up an IPCEI.

238. European Commission Competition Policy, "Joint European Forum for IPCEI (JEF-IPCEI)", European Commission, n.d., accessed on 21 July 2025, https://competition-policy.ec.europa.eu/state-aid/ipcei/joint-european-forum-ipcei_en.

239. European Commission Competition Policy, "Practical information for Important Projects of Common European Interest (IPCEI)", European Commission, n.d., accessed on 21 July 2025, https://competition-policy.ec.europa.eu/state-aid/ipcei/practical-information_en.

240. European Commission Competition Policy, "Approved IPCEIs in the Microelectronics value chain", European Commission, n.d., accessed on 21 July 2025, https://competition-policy.ec.europa.eu/state-aid/ipcei/approved-ipceis/microelectronics-value-chain_en.

241. See: "IPCEI on Microelectronics", https://www.ipcei-me.eu/.

242. European Commission, "State aid: Commission approves up to €8.1 billion of public support by fourteen Member States for an Important Project of Common European Interest in microelectronics and communication technologies", 8 June 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3087.

243. European Commission Shaping Europe's digital future, "European High Performance Computing Joint Undertaking - EuroHPC JU", European Commission, n.d., accessed on 21 July 2025, https://digital-strategy.ec.europa.eu/en/policies/high-performance-computing-joint-undertaking.

244. European Commission Competition Policy, "Approved IPCEI Next Generation Cloud Infrastructure and Services", European Commission, n.d., accessed on 21 July 2025, https://competition-policy.ec.europa.eu/state-aid/ipcei/approved-ipceis/cloud_en.

245. European Court of Auditors, "2023: Annual Report on EU Joint Undertakings for the financial year 2023", European Union, 13 November 2024, https://www.eca.europa.eu/ECAPublications/SAR-JUS-2023/SAR-JUS-2023_EN.pdf.

246. Ibid.

247. Andreas Eisl, "EU industrial policy in the making. From ad hoc exercises to key instrument: how to make IPCEIs fit for the long run", Science Po Institutional Repository (2022), https://sciencespo.hal.science/hal-04616546v1.

248. European Commission Competition Policy, "DG COMP Code of good practices for a transparent, inclusive, faster design and assessment of IPCEIs", European Commission, 17 May 2023, https://competition-policy.ec.europa.eu/system/files/2023-05/IPCEIs_DG_COMP_code_of_good_practices.pdf.

249. See, for example: EUR-Lex, "Council Regulation (EU) 2021/2085 of 19 November 2021 establishing the Joint Undertakings under Horizon Europe and repealing Regulations (EC) No 219/2007, (EU) No 557/2014, (EU) No 558/2014, (EU) No 559/2014, (EU) No 560/2014, (EU) No 561/2014 and (EU) No 642/2014".

250. For example, see: the Clean Aviation (CA) JU, the Circular Bio-based Europe (CBE) JU, and the SNS JU.

251. European Court of Auditors, "2023: Annual Report on EU Joint Undertakings for the financial year 2023".

252. EUR-Lex, "Council Regulation (EU) 2021/2085 of 19 November 2021 establishing the Joint Undertakings under Horizon Europe and repealing Regulations (EC) No 219/2007, (EU) No 557/2014, (EU) No 558/2014, (EU) No 559/2014, (EU) No 560/2014, (EU) No 561/2014 and (EU) No 642/2014", Art. 3(4).

253. For example, as proposed in the case of the LDT CitiVERSE EDIC. See: European Commission Shaping Europe's digital future, "EU-funded AI innovation powers a new era in cooperative smart city development", European Commission, 12 December 2024, https://digital-strategy.ec.europa.eu/en/news/eu-funded-ai-innovation-powers-new-era-cooperative-smart-city-development.

254. Article 1(2) of each of the 3 EC decisions on the EDICs, cited above.

255. European Commission Competition Policy, "Design Support Hub", European Commission, n.d., accessed on 21 July 2025, https://competition-policy.ec.europa.eu/state-aid/ipcei/design-support-hub_en?prefLang=de.

256. European Commission Competition Policy, "Joint European Forum for IPCEI (JEF-IPCEI)", European Commission, n.d., accessed on 21 July 2025, https://competition-policy.ec.europa.eu/state-aid/ipcei/joint-european-forum-ipcei_en.

257. Circular Bio-based Joint Undertaking, "How to apply for funding", European Commission, n.d., accessed on 21 July 2025, https://www.cbe.europa.eu/how-apply-funding#:~:text=for%20the%20topic.-,Who%20can%20apply?,Associations.

258. EUR-Lex, "Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (Text with EEA relevance)", European Union, n.d., accessed on 21 July 2025, Article 3(1)(a), https://eur-lex.europa.eu/eli/dec/2022/2481/oj/eng.

259. See, for instance: Clean Hydrogen Partnership, "Strategic Research and Innovation Agenda", European Commission, n.d., accessed on 21 July 2025, https://www.clean-hydrogen.europa.eu/about-us/key-documents/strategic-research-and-innovation-agenda_en.

260. European Commission Shaping Europe's digital future, "European Digital Infrastructure Consortium - EDIC", European Commission, n.d., accessed on 21 July 2025, https://digital-strategy.ec.europa.eu/en/policies/edic.

261. EUR-Lex, "Commission Implementing Decision (EU) 2024/458 of 1 February 2024 on setting up the European Digital

Infrastructure Consortium for the Alliance for Language Technologies (ALT-EDIC)", Art. 15.

262. EUR-Lex, "Commission Implementing Decision (EU) 2024/1432 of 21 May 2024 setting up the European Digital Infrastructure Consortium for European Blockchain Partnership and European Blockchain Service Infrastructure (EUROPEUM-EDIC)", Art. 11.

263. Living in EU, ""Development of the CitiVerse" call", 8 September 2023, https://living-in.eu/news/development-citiverse-call.

264. European Commission Shaping Europe's digital future, "Over €760 million investment from the Digital Europe Programme for Europe's digital transition and cybersecurity", European Commission, 14 December 2023, https://digital-strategy.ec.europa.eu/en/news/over-eu760-million-investment-digital-europe-programme-europes-digital-transition-and-cybersecurity.

265. EUR-Lex, "Commission Implementing Decision (EU) 2024/1432 of 21 May 2024 setting up the European Digital Infrastructure Consortium for European Blockchain Partnership and European Blockchain Service Infrastructure (EUROPEUM-EDIC)", Art. 11.

266. EUR-Lex, "Commission Implementing Decision (EU) 2024/458 of 1 February 2024 on setting up the European Digital Infrastructure Consortium for the Alliance for Language Technologies (ALT-EDIC)", Art. 10/4.

267. See, for instance: Luuk Schmitz, Timo Seidl and Tobia Wuttke, "The costs of conditionality. IPCEIs and the constrained politics of EU industrial policy", Competition & Change (2025), Sage Journals, https://doi.org/10.1177/10245294251320675.

268. EUR-Lex, "Council Regulation (EU) 2021/2085 of 19 November 2021 establishing the Joint Undertakings under Horizon Europe and repealing Regulations (EC) No 219/2007, (EU) No 557/2014, (EU) No 558/2014, (EU) No 559/2014, (EU) No 560/2014, (EU) No 561/2014 and (EU) No 642/2014", Recital 10.

269. Ibid, Recital 37.

270. European Commission, "What are the main features of an EDIC?".

271. European Commission, "What is an EDIC?".

272. EUR-Lex, "COMMUNICATION FROM THE COMMISSION Criteria for the analysis of the compatibility with the internal market of State aid to promote the execution of important projects of common European interest", European Union, 30 December 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1230(02).

273. Ibid.

274. European Commission Competition Policy, "DG COMP Code of good practices for a transparent, inclusive, faster design and IPCEIs".

275. EUR-Lex, "Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (Text with EEA relevance)", Art. 15(4).

276. Ibid.

277. European Cyber Resilience Act, "Final Text, European Cyber Resilience Act", n.d., accessed on 21 July 2025, https://www.european-cyber-resilience-act.com/Cyber_Resilience_Act_Article_13.html.

278. EUR-Lex, "Commission Implementing Decision (EU) 2024/458 of 1 February 2024 on setting up the European Digital Infrastructure Consortium for the Alliance for Language Technologies (ALT-EDIC)", Art. 31.

279. European Union Agency for Cybersecurity, "NIS2 Technical Implementation Guidance", 26 June 2025, https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance.

280. European Commission, "AI Continent – new cloud and AI development act", n.d., accessed on 21 July 2025, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14628-AI-Continent-new-cloud-and-AI-development-act_en.

281. Daria Rutecka, "The Digital Content Directive and the Sale of Goods Directive: when to apply which?", Schoenherr, 3 January 2022, https://www.schoenherr.eu/content/the-digital-content-directive-and-the-sale-of-goods-directive-when-to-apply-which.

282. ERA-LEARN, "Next Framework Programme (FP10)", n.d., accessed on 21 July 2025, https://www.era-learn.eu/partnerships-in-a-nutshell/european-partnerships/next-framework-programme-fp10.

283. EUR-Lex, "Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (Text with EEA relevance)", Art. 15(4).

284. Ibid, Art. 13(2).

285. The current German Sovereign Tech Agency (Agentur für Sprunginnovationen im Bereich Souveräne Technologien) is a state-owned limited liability company (GmbH) in Germany,

286. European Commission Shaping Europe's digital future, "EU-funded AI innovation powers a new era in cooperative smart city development", European Commission, 12 December 2024, https://digital-strategy.ec.europa.eu/en/news/eu-funded-ai-innovation-powers-new-era-cooperative-smart-city-development.

287. Living in EU, "The LDT CitiVERSE EDIC is a fact!", n.d., 4 March 2024, https://living-in.eu/news/ldt-citiverse-edic-fact.

288. Meanwhile, the ALT-EDIC has a more overt focus on the geographic location of its 'users' and 'industrial consortium,' defining both in its statutes in terms of those who are based in the EU or EEA (Article 1(8), (14)). By contrast, the EUROPEUM-EDIC does not define users.

289. EUR-Lex, "Commission Implementing Decision (EU) 2024/1432 of 21 May 2024 setting up the European Digital Infrastructure Consortium for European Blockchain Partnership and European Blockchain Service Infrastructure (EUROPEUM-EDIC)", Art. 11.

290. EUR-Lex, "Commission Implementing Decision (EU) 2024/458 of 1 February 2024 on setting up the European Digital Infrastructure Consortium for the Alliance for Language Technologies (ALT-EDIC)", Art. 10/4.

291. Catharina Sørensen, "How the frugal four could grow in number and influence", European Council on Foreign Relations, 7 September 2020, https://ecfr.eu/article/commentary_how_the_frugal_four_could_grow_in_number_and_influence/.