31 March 2025

INPUT FOR THE CONSULTATION ON THE NEXT MULTIANNUAL FINANCIAL FRAMEWORK

Securing the EU's Digital Sovereignty and Competitiveness by Investing in Sustainable Open Digital Infrastructure

A Proposal to Invest in Open Source Infrastructure Dependencies and Sustainability in the Next MFF through an EU Sovereign Tech Fund (EU-STF)

A tangible proposal to answer the Warsaw Call

In response to the urgent need for enhanced cybersecurity, as highlighted during the Telecommunications and Information Society (TTE) Council in Warsaw on 5 March 2025, **we propose the establishment of the EU Sovereign Tech Fund (EU-STF), modelled after Germany's Sovereign Tech Agency**. This €54 million initiative directly addresses the call for strengthened cybersecurity measures by focusing on the **security of open source products, the sustainability of open source projects and by extension all software the EU's economy depends on**. By proactively investing in the auditing and maintenance of open source base technologies, the EU-STF will bolster the resilience of our digital ecosystem, aligning with the Warsaw Call's emphasis on cooperation, investment, and preparedness. This approach ensures that the EU takes the lead in cybersecurity in an ever-evolving threat landscape, reinforcing our commitment to a secure and resilient digital future.

The EU-STF is designed to enhance cybersecurity, reduce the need for heavy-handed regulation, and increase trust in Europe's digital ecosystem, thereby laying the foundation for a **sovereign and competitive EU**. By securing open source software, the EU-STF will not only fortify our digital infrastructure but also contribute to the development of a robust cybersecurity framework, ensuring that the EU's digital transformation is underpinned by strong cybersecurity foundations.

Amid growing cyber threats, the EU must consider open source base technologies as digital infrastructure

Securing open source code and open source software (OSS) means securing all our digital infrastructure and addressing systemic risk.

The scale of this need is so high simply because **open source code is integral to the functionality of virtually all digital assets**. Its open nature allows for widespread collaboration and innovation; but like with all software, security must be a priority. The code's openness necessitates particular security measures to protect against exploitation. Investing in the security of open source will have a very high return in terms of inherently bolstering the security of all digital assets that rely on it, creating a more resilient digital environment.

A helpful framing for policymakers thinking about open source software is to think of it as infrastructure, but for all things virtual. No analogy from the physical world is perfect, but parallels have been drawn between open source software's role in society and:

> **Water Management**
> Open source software is 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, open source software requires maintenance that correlates with its criticality and usage. Investment by a few benefits many, and maintenance is crucial to prevent catastrophic failures.[1]

These infrastructures receive attention and funding from policymakers through initiatives like the EU Water and Waste Framework Directives, the European Securities and Markets Authority, and the Connecting Europe Facility and Cohesion Fund. We propose establishing the EU Sovereign Tech Fund (EU-STF), modeled after Germany's Sovereign

[1] For a deep-dive into these analogies, see Stewart Scott, Sara Ann Brackett, Trey Herr, Maia Hamin with the Open Source Policy Network, "Avoiding the success trap: Toward policy for open-source software as infrastructure," Cybersecurity Report, February 8, 2023, accessed at Atlantic Council.

Tech Agency. This €54 million initiative would directly address cybersecurity by focusing on the security and sustainability of open source software, **offering a high-return investment to mitigate systemic risk in the EU**.

This is not just theoretical, as studies have repeatedly shown the **reach and value of open source**. According to the Linux Foundation, an estimated 70-90% of any given software codebase – including those with huge societal applications, like the International Space Station – is made up of open source components. Without OSS and networks of OSS developers, firms would pay an estimated 3.5 times more to build the software and platforms that run their businesses, or roughly **€8.8 trillion**. In terms of Europe itself, **open source is not just a technological asset** – it is an essential pillar of Europe's economy, including its independence, competitiveness, and innovation.

Based on what we know of the value and reach of open source – both in Europe and beyond – **the potential societal and economic impacts of open source vulnerabilities are huge**. And the benefits of increased trust in open source is a cornerstone of all of the EU's digital efforts.

Recent high-profile vulnerabilities in open source, like the XZ Utils backdoor and the log4shell vulnerability in the open source logging tool log4j, have exposed **the imperative need to secure open source code, which is highly prevalent across all our digital infrastructure**. Other incidents, like Solar Winds hack, have underscored the vulnerability of proprietary software, showing that these cybersecurity risks are by no means unique to open source software. On the contrary, open source basic technologies are the foundation of every software application, open and proprietary alike. Investing in the security of these technologies has an outsized impact, because every Euro invested in securing these basic components goes on to improve the cybersecurity of every application that depends on it.

As all of these cyber threats are compounding – and becoming even more resonant in the context of warming geopolitical conditions – the health and security of the open source ecosystem and the infrastructure that depends on it becomes more important than ever before. At the same time commensurate investment and support for open source software is essential to European competitiveness. Below we make the economic and security policy case for such investment from across the public sector; and not just member states, but the European Union itself.

What is Germany's Sovereign Tech Fund?

Germany's Sovereign Tech Fund is a strategic initiative aimed at bolstering digital sovereignty and innovation through targeted investments in open source software. This fund, operated by the Sovereign Tech Agency GmbH, fully owned by the German State, recognises that open source software is the backbone of modern digital infrastructure, essential for technologies ranging from AI to quantum computing. Despite its critical role, open source software often lacks adequate support and investment, posing risks to stability, competitiveness, and security.

Sovereign Tech Agency

The Sovereign Tech Fund addresses this market failure by providing long-term public funding to strengthen foundational digital technologies. These include programming libraries, package managers, communication protocols, developer tools, and encryption technologies. By investing in these core components, the fund aims to prevent digital infrastructure from becoming controlled by a few powerful entities, ensuring a balanced and resilient ecosystem.

The fund's investments are designed to scale across various sectors, benefiting a wide array of users, including startups and small and medium-sized businesses. Enhancing the security, stability, and reusability of open software components directly boosts productivity and innovation capacity.

Backed by a team of experts with diverse backgrounds and extensive connections within the open source community, the Sovereign Tech Fund operates globally to secure open digital infrastructure. This infrastructure is vital for a future-oriented economy and society, much like physical infrastructure such as roads and railways.

The Economic Case: Why should Europe invest in open source to secure its digital infrastructure?

The **strategic initiatives outlined in Europe's digital policy – and by extension *all* of its policy efforts – are heavily reliant on open source code and OSS** as a critical component of its technological infrastructure.

A study commissioned by the European Commission's Directorate-General for Communications Networks, Content and Technology (DG-CNECT) in 2021 highlighted that **companies within the EU invested approximately €1 billion in OSS in 2018, resulting in an economic impact estimated between €65 and €95 billion**. This reflects a hard-to-beat cost-benefit ratio, indicating that open source is not only a technological asset but also a significant economic driver.

Despite the ROI on investing in open source, such technologies are chronically under-resourced by both the public and private sector. **Open source code and software closely follows the trajectory of 'tragedy of the commons' economic model**, one whereby a public good that benefits all is systematically under-funded. Because open source technologies are free to use and freely shared, they enable immense innovation and cost savings for businesses and governments. However, **no single actor has an incentive to ensure its long-term sustainability**.

For example, **the private sector benefits enormously from open source, and yet private investment in its security is inconsistent and insufficient**. The largest open source users – corporations, public institutions, and governments – have the greatest responsibility to ensure its sustainability. But due to the free-rider problem, most companies do not invest in securing the key code and packages they rely on.

This is where public policy must step in. Just as the EU ensures the safety and sustainability of physical infrastructure – like water systems, roads, and bridges – **it must also ensure the security and sustainability of digital infrastructure**. Without proactive investment in OSS security, Europe faces escalating cyber risks and the potential for widespread digital supply chain failures. This threatens nearly all of Europe's potential digital and industrial policy objectives over the next year, as outlined in its latest 2025 work programme.

Historically, major infrastructure failures like bridge collapses trigger sudden investment, but **continuous and routine maintenance remains neglected,** even though it is much more cost-effective and it would help prevent these same crises from happening again. The same applies to open source security: after high-profile incidents like log4shell, there is a

surge of attention and funding, but **long-term maintenance never gets prioritised, particularly for open source, which is underfunded already**.

Ensuring the robustness of open source in this geopolitical environment is paramount for safeguarding Europe's digital infrastructure and, by extension, its economic and strategic interests. It also benefits the entire world, depoliticising open source technology and **showing Europe is a leader in building more open digital markets as it seeks to develop its own sovereign digital infrastructure**.

Sovereign Security: A Strategic Imperative for Europe

Achieving Europe's sovereign security by investing in the open source ecosystem is **cross-cutting for the EU's digital sovereignty, competitiveness, resilience, and economic stability**. The EU Sovereign Tech Fund (EU-STF) would provide a structured investment mechanism to support OSS projects that underpin the European economy, public services, and critical infrastructure. By ensuring that open source remains secure and well-maintained, the EU can enhance economic efficiency while helping European businesses meet cybersecurity compliance requirements (for example under the Cyber Resilience Act) without being overburdened with regulation.

Increasing Digital Sovereignty

Reducing dependencies on digital infrastructures provided by a small number of vendors in concentrated markets is central to the pursuit of digital sovereignty in Europe. The EU-STF plays a direct and indirect role in achieving this goal: 1) all existing and future alternatives, be an an EU Digital Identity Wallet, Open Internet Stack or EuroStack, will be built using open source and need to be trusted to be successful, 2) the EU needs to invest into understanding its core software dependencies, across geographies and industrial verticals.

By proactively funding open source security and maintenance, the EU can:

- Strengthen EU understanding and management capacity of its digital infrastructure, ensuring that critical OSS remains secure and aligned with European priorities.
- Reduce reliance on a small number of software providers, preventing vendor lock-in and reinforcing Europe's open strategic autonomy.

Boosting Economic Competitiveness

The Draghi report on EU competitiveness has emphasised the need for technological independence, but this cannot be achieved without **investment in open source**

sustainability to boost competitiveness. Investment in open source security is a high-return economic strategy, as the European Commission study indicates that every €1 invested in open source generates over €4 in economic benefits, enabling new opportunities for large and small firms alike. When focusing on the security of open source base technologies "upstream" that are dependencies for many companies' and public institutions' software stacks "downstream", the return on investment is likely to be much higher.

By proactively funding open source security and maintenance, the EU can:

- Lower the cost for businesses in meeting security standards without excessive compliance costs.
- Ensure that widely used OSS projects remain available, secure, and accessible to European enterprises and institutions.
- Reduce the need for heavy-handed regulation by addressing security risks at the source.
- Strengthen European innovation and competitiveness through high-quality open source software components to create state of the art software products and services

Strengthening Cybersecurity

The Cyber Resilience Act (CRA) introduces new security obligations for software vendors and users. However, many open source projects lack the resources to meet these requirements, which could inadvertently increase costs for businesses and deter innovation. The CRA is the manifestation of a larger issue though, one wherein **chronic underinvestment in open source puts a greater maintenance burden on open source maintainers**, leading to long-term challenges in security auditing and maintenance. A 2024 survey of open source maintainers, half of which are based in Europe, showed that 60% of maintainers are unpaid, and among unpaid maintainers, the majority are the only maintainer of their project.

By proactively funding open source security and maintenance, the EU can:

- Decrease legal uncertainty and risk for European businesses, especially SMEs that rely on OSS but cannot afford independent security audits.
- Reduce cyber attack response costs for businesses and public institutions, preventing financial and operational losses.
- Attract more OSS experts in Europe — given the trends from the last decades, the need for IT and OSS expertise is and will be immense. The EU-STF would help make Europe competitive in this area.

Preserving Economic Stability

Without sustained investment, **Europe risks supply chain disruptions similar to those caused by vulnerabilities like log4shell**, which impacted thousands of organisations globally. Waiting for a crisis before deciding to act is neither cost-effective nor responsible. Long-term maintenance and security auditing would decrease sudden bursts of investment and be more financially sustainable in the long-term.

By proactively funding open source security and maintenance, the EU can:

- Encourage European businesses and governments to invest in OSS security, fostering a more self-sufficient and resilient digital ecosystem.
- Lower compliance costs for SMEs and startups, enabling them to innovate without excessive security-related regulatory burdens.
- Ensure stability in European supply chains by preventing OSS vulnerabilities from cascading across industries.

PROPOSAL: An EU Sovereign Tech Fund (EU-STF)

The EU should budget for an EU Sovereign Tech Fund (EU-STF) with an initial budget of €54 million. The EU Sovereign Tech Fund (EU-STF) should be established as a dedicated funding instrument to strengthen Europe's digital resilience by ensuring the security and sustainability of critical open source software components. The fund would provide structured financial support to open source libraries and projects that are widely used across the EU's public and private sectors and are essential for economic competitiveness, cybersecurity, and digital sovereignty.

A structured public funding mechanism is needed to fill this public gap in funding for open source maintenance and security, ensuring that:

- Key open source projects are proactively secured, rather than reacting after a crisis;
- Long-term support is provided for widely used software components, reducing systemic risks; and,
- The EU maintains control over its digital infrastructure and secures it through European investment, strengthening its competitiveness and digital sovereignty.

Legal and Policy Basis

The establishment of the EU-STF would **address a structural gap in the EU's technology and cybersecurity funding mechanisms**. While the EU has made substantial investments in research and innovation, there is no dedicated instrument focused on the maintenance and security of open source-dependent infrastructure that underpins Europe's digital economy and society at large. The fund would complement existing regulatory efforts, such as the CRA, by ensuring that security requirements placed on software providers are matched by public investment in key OSS projects that serve as foundational digital infrastructure.

The EU-STF would align with existing EU policy priorities, particularly:

- The Cyber Resilience Act (CRA), by ensuring that OSS maintainers have the financial resources to meet regulatory security requirements.
- The European Competitiveness Agenda, by securing the OSS components that underpin Europe's industrial and digital competitiveness.
- The Digital Europe and Horizon Europe programs, by complementing research and innovation funding with investment in maintenance and cybersecurity.

Responsibilities of the EU-STF

The primary objective of the EU-STF would be to **ensure the long-term security and sustainability of OSS components that are widely used in European public services, industries, and critical infrastructure**. To achieve this, the fund would focus on four core actions, namely:

1. **Identifying critical digital infrastructure in the EU that is dependent on open source components and mapping those dependencies**

The first step to ensuring digital sovereignty is to comprehensively map out the software dependencies used across critical infrastructure and public services within the EU, in order to understand which ones are vulnerable to cyber threats related to vulnerabilities or issues in maintenance. This includes not only proprietary software but also open source components that are widely integrated into essential systems. 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.

2. **Evaluating and enhancing security frameworks of those dependencies to determine possible security vulnerabilities and prioritise open source components for investment**

Once dependencies are identified, rigorous security audits must be conducted to assess their integrity, security posture, and overall resilience against cyber threats. These audits would involve code reviews, vulnerability testing, and compliance checks with EU cybersecurity standards. By proactively identifying weaknesses, the EU can mitigate security risks before they can be exploited, ensuring the safety and stability of digital systems. It can then create a mechanism to help match appropriate funding and resources to support investment in the components identified as having dependencies. ***Note that it is crucial that the EU-STF follows the model of the German STF closely. We propose a structured approach to evaluating and enhancing security frameworks, ensuring that assessments are actionable and aligned with the needs of open source maintainers, rather than relying on generic consultancies.***

3. **Invest in the maintenance and strengthening of key open source components**

For dependencies found to have security gaps or maintenance issues, the EU Sovereign Tech Fund should strategically invest in their development and support. This could involve funding patches, updates, or even the employment of dedicated maintainers for critical open source projects. By investing in the sustainability and security of essential software,

the EU ensures long-term digital resilience and reduces reliance on third-party entities that may not prioritize European security needs.

4. **Invest in Ecosystem-Strengthening Activities**

To strengthen the open source ecosystem, the EU-STF should be responsible for coordinating with national cybersecurity authorities to align efforts, share threat intelligence, and enhance cross-border cooperation, ensuring a unified approach to securing critical digital infrastructure. Maintenance funding should not be duplicated. It should also foster collaboration between OSS maintainers, industry, and public institutions to create sustainable support networks, facilitate knowledge exchange and seek to match public and private funding. Additionally, the EU-STF should develop training programs to equip maintainers and developers with secure coding practices and vulnerability management skills, reinforcing the resilience of open source projects and bolstering Europe's digital sovereignty.

Objectives of the EU-STF

Mapping OSS Dependencies

- Conduct a systematic assessment of which OSS projects are most critical to European digital infrastructure
- Identify high-impact, widely used software components across key economic sectors, including finance, telecommunications, energy, and public administration
- Develop an ongoing monitoring mechanism to track security risks and funding needs in the OSS ecosystem

Auditing Security Risks

- Establish a dedicated framework to assess vulnerabilities in high-impact OSS projects and evaluate their security posture
- Provide targeted funding for security audits, vulnerability remediation, and compliance measures
- Support maintainers and developers in meeting the security requirements introduced by the Cyber Resilience Act (CRA)

Funding Long-Term Maintenance

- Develop a structured funding mechanism that provides direct financial support to maintainers and organizations working on critical OSS projects.
- Ensure that funding is flexible, responsive, and adapted to the needs of different OSS projects, ranging from individual developers to larger community-driven initiatives.
- Prioritise sustained funding rather than one-off grants, ensuring long-term security and sustainability.

Invest in Ecosystem-Strengthening

- Coordinate with national cybersecurity authorities to align efforts, share threat intelligence, and enhance cross-border cooperation
- Foster collaboration between OSS maintainers, industry, and public institutions to ensure sustainable support and knowledge exchange
- Develop training programs to equip maintainers and developers with secure coding practices and vulnerability management skills

Next Steps for the Establishment of the EU-STF

The EU-STF would draw on lessons from Germany's Sovereign Tech Fund (STF), which has now evolved to a programme of the Sovereign Tech Agency (STA). The STF has successfully demonstrated that public funding can be effectively structured to support critical OSS projects while maintaining operational flexibility and community engagement. Key elements of the STF that could inform the design of the EU-STF include:

- A One-Stop-Shop funding approach that minimizes administrative burden for OSS maintainers and ensures that financial support is distributed efficiently and transparently.
- 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.
- A balance between proactive and reactive funding to allow for both long-term investment in critical OSS infrastructure and rapid response to emerging security risks.

EU-STF Feasibility Study

Building on the German STA success, OpenForum Europe – together with Fraunhofer ISI and Professor Thomas Streinz of the European University Institute – are currently conducting a detailed feasibility study on the potential structure and impact of an EU Sovereign Tech Fund, which will be released at the end of June. It will feature **both an economic analysis and a legal analysis**.

The economic analysis would consider how the high direct return-on-investment and increased economic growth will contribute concretely to the European agenda, including competitiveness and digital sovereignty. The legal analysis would consider what the mandate of a funding instrument could be tasked with tackling these objectives, and to consider what the contribution of the EU-wide STA would be, from both the economic and legal perspectives.

OFE is a not-for-profit, independent European based think tank which focuses on openness within the IT sector. OFE draws its support from a broad range of stakeholders committed to openness: Among them leading global ICT technology providers, European SMEs, user organisations, the openness academic community represented by the OpenForum Academy and the wider openness community. Tapping into this broad basis for support provides OFE with expertise across all major ICT topics, including applying its knowledge to the evolving technologies such as artificial intelligence, blockchain, cloud computing and IoT. Views expressed by OFE do not necessarily reflect those held by its supporters.

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: Boulevard Charlemagne 96, 1000 Brussels, Belgium
Web: openforumeurope.org
e-mail: info@openforumeurope.org

OpenForum Europe