Discussion Paper

Market-Oriented Funding Structures for the Open Source Software Ecosystem

Analysis of the current state of open source software and a proposal for financing professional development structures and adequate cybersecurity measures

Authors: Dr. sc. ETH David M. Sommer, Florian Kubiak, Dr. Raphael M. Reischuk

Executive Summary

Digital infrastructures are a central foundation for administration, the economy, and society. With the increasing use of software and cloud technologies, structural security issues are becoming more prominent, particularly with regard to the confidentiality of sensitive data and the availability, integrity, and resilience of the underlying infrastructures.

As has become apparent repeatedly in recent times, the software and cloud technologies used in Switzerland and in the European Union show structural security deficits. These deficits are posing a strategic risk to Europe given the growing complexity of infrastructure, increasing dependencies in supply chains, and new regulatory requirements.

This discussion paper examines strategic options for mitigating such deficiencies by fostering alternatives based on open software and open digital communication protocols. The aim is to identify the fundamental requirements for innovative, security-robust, and sustainably controllable solutions and to develop strategic, regulatory, and infrastructural frameworks for their realisation.

The discussion paper also analyses the market requirements for open software components and companies, which are collectively referred to as open source software (OSS). A characteristic feature of OSS is its freely accessible source code, which enables its use, further development, and distribution by a broad range of actors. Building on this, the report presents a structured overview of existing projects and initiatives for the long-term financing and strengthening of OSS ecosystems by companies, private individuals, and government institutions.

The results of the analysis reveal a significant **discrepancy between the high relevance and use of open source software** on the one hand and the **extent of the financial and organisational resources available for this purpose** on the other. This underfunding tends to jeopardise innovation, the professionalisation of development processes, and compliance with appropriate cybersecurity standards. It is therefore urgent to explore and implement existing and new financing options for open source software.

As a solution, coordinated funding structures are proposed to specifically strengthen and further develop the existing OSS ecosystem. Key components of these funding structures comprise clearly defined roles for public institutions and philanthropic foundations, as well as mechanisms to systematically ensure an adequate degree of cybersecurity compliance, long-term adaptability, and the strategic further development capabilities of the technologies.

—

This discussion paper was made possible by the Mercator Foundation (focus on supporting responsible tech) and the Swiss National Test Institute for Cybersecurity NTC (focus on security testing of software and infrastructure). The authors would like to thank Christian Folini and Vlad-Stefan Harbuz for their critical review of the manuscript and their valuable suggestions.

Contents

1 Introduction

The European IT infrastructure is largely based on platforms and services provided by a small number of market-leading providers. As these providers are predominantly based outside of Europe, this creates dependencies that can impair Europe's ability to make decisions and take action at a technological and political level. Recurring security incidents also underscore the fact that established technologies do not always meet the requirements for an adequate level of cybersecurity. While in the past the risks of outsourcing were considered acceptable overall due to the comparatively low threat level, recent international developments are fueling the discussion about a dedicated European IT infrastructure.

As a result, the desire for available alternatives is growing louder. According to a Bitkom survey conducted in December 2024[1], 92 % of German companies want greater independence from the US, 96 % are in favor of greater digital sovereignty, and 86 % want a European hyperscaler. According to a report by the NTC from December 2024[2], 95 % consider the current dependencies to be dangerous and 90 % would like to see a Swiss or European hyperscaler. The Draghi Report on EU competitiveness from September 2024[3] warns that Europe imports 80 % of its digital technology and proposes targeted economic development efforts.

A sustainable alternative to closed software and international dependencies is the use and targeted fostering of open source software (OSS), which is already a fundamental part of the modern software landscape. OSS is included in 97 % of the software scanned by Blackduck[4]. These are often central building blocks that, in their sea of design forms, are usually supported by only a few individual software developers and, due to their focus on maximum functionality, often neglect cybersecurity measures. Together with the Swiss Federal Office for Cybersecurity (BACS), the NTC has shown that targeted testing can strengthen the security of OSS and increase Switzerland's cyber resilience[5]. Sustainable maintenance of the essential building blocks is becoming increasingly necessary in order to provide a resilient infrastructure and mitigate the risks discussed.

Given the growing relevance of open source software for alternatives in the European software and hardware landscape, this discussion paper examines options for specifically promoting market-compatible OSS ecosystems. A particular focus is placed on the availability, confidentiality, and integrity of IT solutions. By specifically incorporating market requirements into the development and promotion of open source software, Europe can address the associated challenges, reduce operating costs, and ensure innovative adaptation to changing needs. A clear strategy is needed to close the supply gap between open infrastructures and lucrative end-customer products, with a focus on sustainable financing and professional development structures.

Motivation of the actors involved. With this discussion paper, the Mercator Foundation Switzerland supports the evaluation of an essential aspect of the digital maturity of Switzerland and Europe and aims to contribute to the establishment of responsible technology. In addition, the NTC is increasingly focusing on the general security of insufficiently tested digital solutions, including open source software. The NTC is committed to ensuring that technologies are secure by promoting the

[1] https://www.bitkom.org/Presse/Presseinformation/Tech-Unternehmen-fordern-Unabhaengigkeit-USA

[2] https://www.ntc.swiss/hubfs/20241216-kurzbericht-systemabhaengigkeiten-ntc-de.pdf

[3] https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en

[4] https://www.blackduck.com/content/dam/black-duck/en-us/reports/rep-ossra.pdf

[5] https://www.ntc.swiss/aktuelles/2025-reports-oss-bacs

integration of cybersecurity as a fixed development and testing step, and also conducts such tests itself.

Geographical perspective. This discussion paper is primarily written from a Swiss perspective and is aimed at Swiss stakeholders from politics, business, and civil society. However, many of the challenges described are European or global in nature — OSS ecosystems are not bound by national borders, and measures often only have an effect in conjunction with European partners. This discussion paper does not systematically distinguish between these levels, which should be understood as a limitation. A more detailed elaboration should explicitly clarify which measures can be implemented at the national level, which require European coordination, and which can only be effective in an international context.

2 Current challenges

The majority of companies and government institutions rely on software solutions for their operational processes that are either directly or indirectly dependent on large, non-European tech companies. These dependencies lead to concrete challenges in practice: Risk analyses[6] warn of loss of data control, limited data sovereignty, and difficulties in assessing security and compliance risks, as the software stack of many providers often remains a black box. The internal measures taken by providers are often opaque[7] and fundamentally difficult to control. The unavailability of essential services, as experienced[8] by Nicolas Guillou, a judge at the International Criminal Court, is also becoming a core risk.

In addition, monopolistic providers can raise prices at will due to a lack of software alternatives and discontinue SaaS services without warning. Infrastructure and software operators have full control over data flow and could allow sensitive data to leak, e.g. via the US CLOUD Act[9]. Geopolitical changes may occur faster than alternatives can be created. When migrating data to new systems, there is a risk that stored data cannot be extracted completely. Proprietary data formats and interfaces further reinforce this vendor lock-in effect and make it considerably more difficult to switch providers.

These challenges are central and arise, among other things, from the fact that Europe does not provide a sufficiently large share of the hardware and software infrastructure used and that it does not exercise strong governance over these central parts of the technology stack.

2.1 Market needs

The causes of the challenges discussed above result, among other things, from the requirements of the private sector market and public procurement for software technology and infrastructure. Companies and government agencies have the following fundamental requirements, with varying relevance depending on the industry and sector:

Cost: Focus on cost-effective solutions, including product introduction and data migration, operation, customisation, and decommissioning.

Availability: Sufficient availability of software and services such that business processes are minimally impacted.

Feature scope: Ease of integration into the existing IT structure with the necessary access functions and scalability, as well as adaptability to new requirements.

[6] https://www.bcg.com/publications/2025/sovereign-clouds-reshaping-national-data-security

[7] https://www.sciencedirect.com/science/article/abs/pii/S0167404823005321

[8] https://www.lemonde.fr/en/international/article/2025/11/19/nicolas-guillou-french-icc-judge-sanctioned-by-the-us-you-are-effectively-blacklisted-by-much-of-the-world-s-banking-system_6747628_4.html

[9] https://dnip.ch/2025/02/27/die-cloud-als-spielball-der-winde/

Support options: Contractually guaranteed, long-term support for operation, migration, and use.

Maintenance and further development: Ensuring continuous product maintenance and adaptation.

Data sovereignty: Control of sensitive data and trade secrets in accordance with data protection regulations.

Certifications: Requirements for providers, such as ISO/IEC 27001 for information security.

Exit strategy: Consideration of switching options to avoid vendor lock-in.

Cybersecurity: Compliance with modern security requirements, regularly tested and improved.

Only a few providers fully meet the above requirements. Established major providers such as Microsoft or Google cover large parts of these requirements – in particular, functionality, support, and availability – but have significant gaps in data sovereignty, exit strategy, and comprehensible cybersecurity. European and open source-based alternatives often meet the requirements for openness and data control, but frequently fail due to a lack of support structures, certifications, or insufficient functionality for enterprise use. As a result, alternatives rarely establish themselves. This is reinforced by network effects: the more widespread a software is, the more attractive it becomes to other users —- not because of its technical quality, but because of the shared infrastructure and common knowledge base. Companies can simply assume that new employees are familiar with widely used software such as Microsoft Office, which reduces training costs and the time needed to get new employees up to speed. The ease of collaboration with customers and partners who use the same tools also reinforces this effect. This makes it difficult for alternatives to gain a foothold, despite technical or sovereignty-related advantages.

The cost argument in particular is only superficially obvious: for example, the US and China systematically invest in their IT industries, thereby generating a considerable competitive advantage for their companies over providers who have to finance themselves purely from the market.

2.2 Challenges in the corporate market

A lack of willingness to invest and courage to innovate has led to a shortage of suitable software alternatives in the corporate market: software development is comparatively cost-intensive, but the marginal costs of hosting the software are minimal. Even in large markets, there are often only a few providers. Small companies can hardly compete with established products and have to specialise in niches. The more financially powerful competitors often buy up competitors while they are still in the development stage. Available support and distribution networks, such as those of Microsoft, offer a major competitive advantage, while even giants like Apple are hesitant or completely absent from the corporate market. In addition, decision-makers prefer established products in order to minimise personal career risks. These market dynamics make it unlikely that viable alternatives will emerge solely through private initiative. Without targeted political support – such as through public procurement decisions, start-up financing, or regulatory frameworks – it will be difficult to break through the existing market powers. This also applies to Switzerland, which has so far has not set its mark in this area.

3 A possible alternative: open source software

The term open source software (OSS) covers different contexts and license forms. This discussion paper deliberately uses a vague definition, which includes the following points:

Accessibility: Source code is freely available for viewing, use, and modification.

Collaboration: Developers and users work together, with the results flowing back into the project for everyone.

Transparency: Software is transparent and understandable for users and programmers, using open protocols for high interoperability.

Adaptability: Software can be adapted and further developed, even in inactive projects; forking (the permitted copying and separate further development) is central to this.

Licensing: Licenses guarantee the free use and modification of open source software, although these guarantees are weakened for commercialisation at times.

3.1 Challenge: OSS and market deficiencies

The community spirit of OSS projects often contrasts with the profit and exclusion logic of commercial projects, which often leads to competitive disadvantages for OSS. Instead, OSS projects share a collaborative spirit: developments are shared through open access to the source code. The open source definitions of the United Nations[10] and the Open Source Initiative[11] promote transparency, although the strong requirements can limit the spread of the license. The focus on community also conflicts with commercial profit interests, leading to funding bottlenecks for OSS. Nevertheless, according to Black Duck Security Reports[12], OSS components are included in 97 % of scanned software, and an average of 70 % – and often more than 90 % – of the software components in applications are OSS.

The paradigm shift and collaborative approach of open source software often improves software quality and enables better integration. OSS components can be operated independently and reduce vendor lock-in risks. Their availability promotes innovation and rapid infrastructure creation. OSS is economically viable for shared needs, but not for niche functionality where few buyers are interested. Despite initial costs, long-term savings are possible: A study by Harvard and the Linux Foundation[13] states that companies would have to spend 3.5 times more on software than they currently do if OSS did not exist. It optimistically[14] estimates the value of the OSS demand side at $8.8 trillion. In addition, 96 % of the value on the demand side is created by only 5 % of OSS developers.

3.2 Challenge: OSS and market deficiencies

There is a significant discrepancy between the widespread use of OSS in software engineering and its limited use among end users, as illustrated in fig. 1. High-quality OSS such as development tools and libraries are available for tech-savvy users. However, user-oriented software and enterprise solutions, such as CRMs and ERPs, are less developed in the open source world. Financial interests stimulate areas such as operating systems and cloud management with hyperscalers. While the infrastructure cores are open, large providers deliberately keep the profitable services built on them – such as AI platforms, auto-scaling, or managed databases – proprietary.

These higher-value components are what retain customers and generate revenue; they are therefore not released as OSS.

Currently, OSS has the following shortcomings compared to commercial closed source software:

[10] https://unite.un.org/en/news/sixteen-organizations-endorse-un-open-source-principles

[11] https://opensource.org/osd

[12] https://www.blackduck.com/content/dam/black-duck/en-us/reports/rep-ossra.pdf

[13] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4693148

[14] https://openpath.quest/2024/questioning-the-value-of-open-source-software/

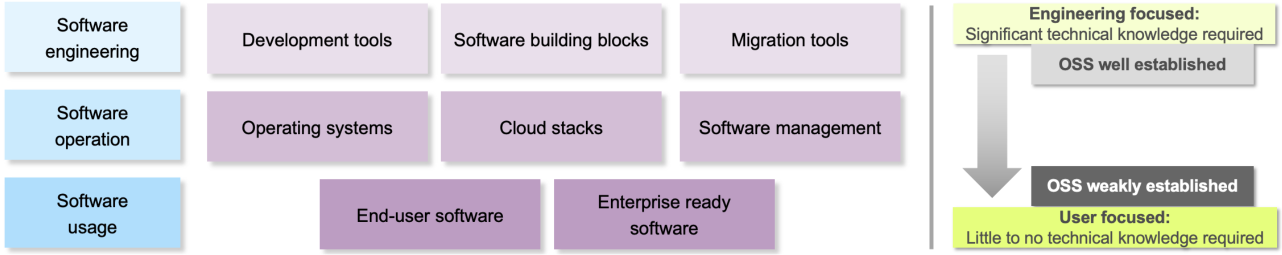

Figure 1: A highly simplified overview of different types of software to illustrate the various areas of OSS application. As a general rule, the closer to the software programmer, the better the OSS landscape works.

Competitive disadvantage: OSS is often available free of charge and does not generate any direct commercial revenue. In addition, OSS is sometimes used commercially in violation of license terms.

Lack of monetisation: The financing options for development and sales activities are limited, e.g., in the Open Core[15] model.

Lack of professionalisation: Quality assurance, sales, alignment with other players, and security infrastructure are often lacking.

Lack of enterprise features: Solutions developed from hobby projects often follow a single-user perspective and do not offer modern IT integrations such as user management or audit functions.

Poor usability: OSS is often not intuitive to use and lacks convenience features.

Lack of synergy effects: Established commercial software offers comprehensive platform support, whereas community-supported OSS products often do not.

Lack of support: Support contracts and reliable help are difficult to arrange due to a lack of experts and legal structures.

Low fault tolerance: Small teams or one-person projects are vulnerable to staff drop-out.

Developer/maintainer burnout: High levels of commitment in small teams without financial compensation lead to overload more quickly.

Lobbying against OSS: Companies avoid competition by preventing open alternatives.

AI-generated attack surface: OSS projects are increasingly confronted with automatically generated vulnerability reports and pull requests from AI systems. Since the quality of these inputs is often difficult to assess, this results in considerable additional effort for triage and review — a burden that quickly overwhelms small maintainer teams. Daniel Stenberg, lead developer of curl, has publicly described and documented[16] this problem.

Open source software is often only funded by companies once it is sufficiently large and relevant, which is the case for projects such as the Linux kernel, but often not for widely used OSS libraries and software. OSS, on the other hand, is worthwhile for promoting software distribution. Consequently, a key challenge is to bridge the funding gap until sufficient relevance is achieved. For companies and public procurement, it is not so much the model (open vs. closed) that is decisive, but rather the contractually guaranteed support services, which are often insufficient or non-existent with OSS.

[15] https://fcl.dev/

[16] https://daniel.haxx.se/blog/2024/01/02/the-i-in-llm-stands-for-intelligence/

Microsoft is regularly discussed critically in various communities, but can serve as a point of reference in terms of its market positioning. The company is particularly successful in the corporate market because it combines its software with a wide range of services and support, which are a decisive factor for many companies.

It is estimated that the majority of open source software[17] is developed by only about 3'000 to 5'000 developers[18], compared to 23.7 million developers worldwide[19]. According to the authors' assessment, these developers are highly qualified, meaning that it is unrealistic to expect such high performance from average software developers. Nevertheless, the estimate makes it clear that considerable progress can be achieved with sufficient political will. Since the majority of the OSS foundation is supported by such a small group, a targeted increase of a few hundred additional, highly qualified developers would have a disproportionately large effect. Measured against the total number of software developers worldwide, this is a modest economic investment — with potentially significant leverage.

3.3 Goals of the license models

Software licenses regulate the use of source code as well as the executability and modification of programs. In the open source community, there are models such as copyleft, which binds modifications under the same license, and free use, which allows free modification. In principle, licenses should respect the interests of developers and users, and protect existing business models.

In the open source world, there are also licensing models that restrict copyleft and free use due to commercial needs: Open Core[15] methodologies offer basic versions free of charge and charge fees for advanced features. Approaches such as Fair Code[20] restrict commercial use, while Fair Source[21] delays publication. Fair Core[15] follows the Open Core mentality with a license that somewhat restricts the use and availability of the Open Core. Post-open source[22]requires fees for commercial ventures.

A review of licensing practices is necessary[23] to improve commercial usability in line with legal definitions and make open source software more financially sustainable.

4 Financing of OSS

The financing of the OSS landscape does not follow a simple principle. Various private, government, and commercial actors pursue their particular interests by contributing according to their own capabilities. This does not represent a sustainable, market-oriented concept[24].

This chapter first outlines the financing options and then discusses specific, existing financing schemes based on private individuals, foundations, companies, and government actors.

4.1 Financing Options

The following section lists important options for financing OSS projects. A basic distinction is made between seed funding and ongoing maintenance. European investments are more cautious with the

[17] https://opensourcefundingsurvey2024.com/

[18] https://openpath.quest/2024/funding-the-five-thousand/

[19] https://www.statista.com/statistics/627312/worldwide-developer-population/

[20] https://faircode.io/

[21] https://fair.io

[22] https://www.theregister.com/2023/12/27/bruce_perens_post_open/

[23] For a detailed discussion see https://dirkriehle.com/2024/07/11/a-plea-for-an-open-source-cloud-copyleft-license/

[24] https://openpath.quest/2024/the-open-source-sustainability-crisis/

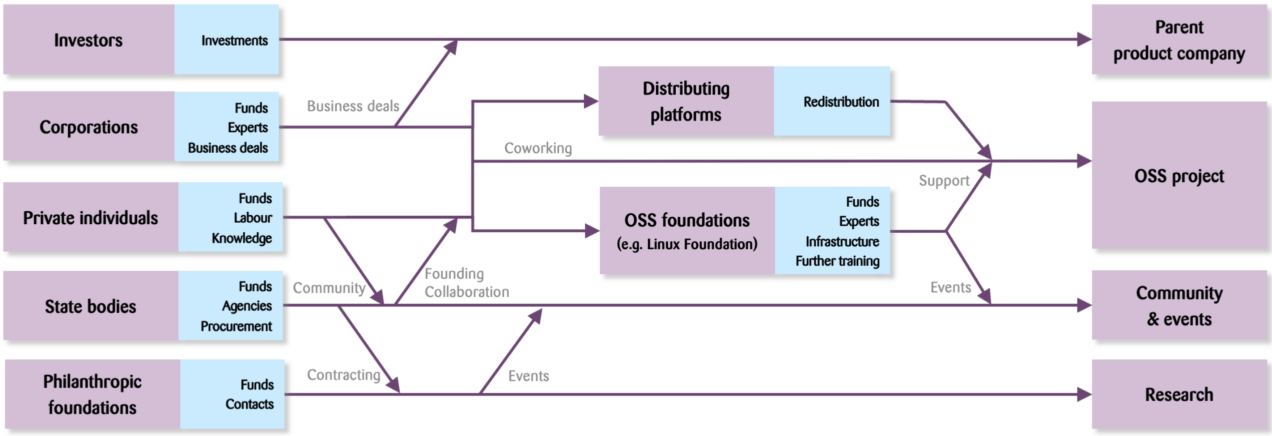

Figure 2: Illustration of the flow of available funds through the OSS landscape. Financial resources flow through each arrow.

former because they are risky from a single project perspective.

Self-initiative/Equity: Developers start projects out of self-interest, often without further growth.

Investment based on product relevance: Companies invest in OSS products in their supply chain, often minimally and primarily for their core interests, usually in the form of programmer working hours, rarely financially.

Business model support: Companies release proprietary tools and products for commercial reasons, see commoditisation of complements[25].

Venture capital: Funding development with the primary goal of generating monetary profit. Rare in the conservative European market, despite the potential for high returns[26].

Crowdfunding: Community funding for projects or specific features (bounty program).

Government innovation programs: Funding through programs such as the Sovereign Tech Fund[27] or Horizon Europe[28].

Distribution organisations: Donations are collected and distributed to developers.

SaaS versions: Cloud-based operation of the software and revenue from the sale of access to the software.

Business version/license: Basic version free of charge, professional version subject to a fee, often referred to as Open Core[15]; see section 3.3.

Paid support/service: Revenue is generated through services provided in connection with OSS products.

Strategic partnerships: Cooperation to achieve common goals, including sponsorship.

Government procurement: Inclusion of OSS as a selection criterion in tenders, such as in the relatively new Swiss EMBAG[29], to increase demand and thus generate funds for development.

[25] https://gwern.net/complement

[26] https://www.toptal.com/management-consultants/venture-capital-consultants/open-source-software-investable-business-model-or-not

[27] https://www.sovereign.tech/de

[28] https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/horizon-europe_en

[29] See *Federal Act on the Use of Electronic Means to Fulfil Government Tasks*, https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/open_source_software/hilfsmittel_oss.html

Particularly noteworthy here is the principle of public money, public code[30], which requires the opening up of publicly funded software.

Foundations and associations: Support from organisations (e.g., Linux Foundation[31], Apache Software Foundation[32], OWASP[33], Eclipse Foundation[34]).

External supporters: A variety of individual contributions such as donations or work performed.

Decisive factors in the acceptance of monetary contributions by participants in the ecosystem are the risk taken, the return on investment (ROI), the voluntary nature of the contribution by users, and the opportunities for users and developers to contribute to the decision making processes.

4.2 Realised financing schemes

The contributions to OSS outlined in fig. 2 are examined in more detail below.

4.2.1 Foundations as financiers

Foundations are either technically oriented (e.g., Linux Foundation[35]), investing their funds directly in projects or in technical personnel, or philanthropic, less technical with a focus on financial support, groundwork, and events. Security awareness in the OSS world has increased since Heartbleed[36] (2014), leading to the establishment of the Open Source Security Foundation[37], which invests $30 million annually in OSS security and organises meetings with major stakeholders. This initiative is part of the Linux Foundation.

4.2.2 Private individuals as financiers and distribution platforms

Private individuals promote OSS through their own projects, voluntary community work, code reviews, and knowledge exchange in internet forums (e.g. Stack Overflow[38]). Projects can be supported in a targeted manner, but little-known yet important projects often go unnoticed. There are platforms that distribute donations directly to projects and disclose how they are used.

The following platforms offer a selection for private individuals and foundations:

GitHub Sponsors: Automatically distributes funds to software dependencies, benefiting multiple projects. [39]

OpenCollective: Simplifies organisational processes, hosts open source projects, but cannot distribute funds; however, it can receive and manage donations for projects.[40]

Tidelift: Analyses and finances software supply chains (is profit-oriented, acquired by Sonar).[41]

thanks.dev: Supports financial distribution to your own software dependency chain.[42]

[30] https://publiccode.eu

[31] https://www.linuxfoundation.org

[32] https://apache.org

[33] https://owasp.org

[34] https://www.eclipse.org/org/foundation/

[35] https://www.linuxfoundation.org

[36] https://en.wikipedia.org/wiki/Heartbleed

[37] https://openssf.org/

[38] https://stackoverflow.com/questions

[39] https://github.com/sponsors

[40] https://opencollective.com/

[41] https://tidelift.com/

[42] https://thanks.dev/

Liberapay: Enables donations to projects and private developers.[43]

How funds can be distributed fairly and efficiently is complex and without a concrete solution. Democratic principles and targeted distribution can provide temporary solutions, taking into account complexity, frequency of use, and security risks. Organisations such as The Open Source Endowment[44] are working on this. Approaches such as Built With[45], bindep[46], and Ecosystem Dashboards[47] use metrics for complexity and distribution. Also notable are Contributor Tiers[48] and funding.json[49]. An EU report[50] recommends a clear division of tasks and rotating experts.

4.2.3 Companies as financiers

In addition to the voluntary work of developers, investments by large companies are also relevant. They invest through their own projects, financial resources, or paid working hours. According to a study by the Linux Foundation and Harvard Business School[17], 86 % of total corporate engagement in OSS is accounted for by paid working hours, i.e. employees who are employed by companies and invest part of their working time in OSS projects. This corresponds to approximately $7.7 billion per year. Direct financial contributions to projects, on the other hand, account for only a small portion. Nevertheless, only little flows into software security, and the original developers and marketing aspects are hardly taken into account. Significant contributions by companies to the OSS world are their own projects such as Kubernetes, React, or AI models (LLMs), which are made available to the public.

For companies, there are foundations and initiatives such as the Open Source Pledge[51]: companies voluntarily commit to donating $2'000 per year per developer to used open source software, which brought in around $3.5 million in 2025.

4.2.4 Government projects as financiers

Government projects for autonomy and OSS exist at the national, international, EU, and UN levels. The UN offers guidelines[52] for open software.

The EU promotes cybersecurity, -sovereignty, and economic competitiveness. It conducts studies on the impact of open-source technologies[53] and the development of funding for critical software[54]. The Gaia-X[55] project lays the foundation for a European cloud. Subsidies are provided through Horizon Europe[28] and EIC Pathfinder.

There are societal demands to intensify these efforts. Significant initiatives include the EuroStack

[43] https://liberapay.com/

[44] https://endowment.dev

[45] https://builtwith.com

[46] https://codeberg.org/vladh/bindep

[47] https://blog.ecosyste.ms/2025/09/25/ecosystem-dashboards.html

[48] https://typescript-eslint.io/maintenance/contributor-tiers/

[49] https://www.fundingjson.org

[50] https://interoperable-europe.ec.europa.eu/sites/default/files/news/2022-04/Development%20of%20a%20Funding%20Mechanism%20for%20Sustaining%20Open%20Source%20Software%20for%20European%20Public%20Services.pdf

[51] https://opensourcepledge.com/

[52] https://unite.un.org/en/news/osi-first-endorse-united-nations-open-source-principles

[53] https://op.europa.eu/en/publication-detail/-/publication/29effe73-2c2c-11ec-bd8e-01aa75ed71a1/language-en

[54] https://interoperable-europe.ec.europa.eu/sites/default/files/news/2022-04/Development%20of%20a%20Funding%20Mechanism%20for%20Sustaining%20Open%20Source%20Software%20for%20European%20Public%20Services.pdf

[55] https://gaia-x.eu/

[56] https://eurostack.eu/the-letter/

movement[56] and the Open Forum Europe's call to expand the German Sovereign Tech Fund[27] to the European level[57]. Nationally, it has been successful in financing IT projects, as has the Sprind-D project[58] for founding innovative start-ups.

Other notable projects and efforts at the national level in the software sector include OpenDesk[59]/ZenDiS[60]/BOSS[61]/NetzwerkSDS[62] and the DINUM projects[63] Etalab[64], the Matrix[65] chat protocol, and the government chat Tchap[66] based on the latter, which unfortunately serves as an example of the need for security reviews[67].

Projects such as the Deutschland-Stack[68] and the French *logiciels libres et communs numériques*[69] are narrowly focused. Despite their monetary impact, they have a structural weakness: funding is tied to a predefined catalog of approved software. New or innovative projects must go through lengthy admission processes before they even become eligible for funding — a significant disadvantage compared to the rapid innovation dynamics of the free market. In addition, government agencies often do not have a complete overview of which OSS components are actually used in their systems. Without this knowledge, targeted funding is hardly possible. Systematic monitoring of the software used – for example, in the form of a Software Bill of Materials (SBOM) – would be a basic prerequisite for effective and market-oriented funding.

In security-critical areas in particular, there is a trend toward the use of open alternatives: for example, the Austrian Armed Forces recently switched from MS365 to an open alternative[70], and the Swiss Army appears to have a comparable stance[71].

Despite higher confidentiality requirements, internal data is repeatedly stored on non-European servers[72] by governments. This has given rise to initiatives such as the Dutch *Rijkscloud*[73] for national cloud platforms.

The EuroStack recommends that the European Commission adopt a policy focus on promoting European IT companies across the stack from hardware to data management.

4.3 Seed funding is needed

The most important findings are as follows. The problem of overworked maintainers[74] has been

[57] https://eu-stf.openforumeurope.org/

[58] https://www.sprind.org/

[59] https://www.opendesk.eu/

[60] https://www.zendis.de/

[61] https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/standarddienste/bueroautomation/poc-boss.html

[62] https://netzwerksds.ch/

[63] https://www.numerique.gouv.fr/numerique-etat/dinum/

[64] https://www.etalab.gouv.fr

[65] https://matrix.org/

[66] https://tchap.numerique.gouv.fr/

[67] https://securityaffairs.com/84219/breaking-news/hacker-broke-tchap.html

[68] https://deutschland-stack.gov.de/

[69] https://code.gouv.fr/fr/plan-action-logiciels-libres-et-communs-numeriques/

[70] https://www.derstandard.at/consent/tcf/story/3000000288311/microsoft-wird-ausgemustert-bundesheer-wechselt-zu-libreoffice

[71] https://www.republik.ch/2025/10/31/der-armeechef-stemmt-sich-gegen-microsoft

[72] https://www.bankinfosecurity.com/eu-commission-microsoft-appeal-edps-office-365-decision-a-25327

[73] https://digitalpolicyalert.org/change/13766-establishment-of-government-cloud-system-rijkscloud

[74] https://mirandaheath.website/report-on-burnout-in-open-source-software/

[75] https://www.jetbrains.com/lp/devecosystem-2023/

known for some time: 73 % of OSS developers[75] have already suffered burnout in their careers, and numerous initiatives are attempting to counteract this. Many projects are developing support models, while companies are providing new functionalities and publishing programming frameworks in order to help shape technological developments and market standards and thus secure market advantages. Foundations such as the Linux Foundation and government actors are increasingly promoting security measures and seeking sustainable financing and governance models — not least in response to the Heartbleed bug[36] .

At the same time, governments are showing growing interest in autonomous and resilient cloud and government infrastructures. Corresponding projects are being created, but they are underrepresented and underfunded.

The first conclusion is that the gap between server infrastructure and end-customer products must be closed. While server infrastructure already relies heavily on open-source technologies, it is in end-customer products, where most of the economic value is created. In order to fund the OSS landscape from usage fees, seed funding must be raised at the outset and a sustainable cash flow model must be developed.

5 Relevance of cybersecurity

Insufficient investment in cybersecurity leads to economic losses in the billions[76] and increasing ransomware attacks[77] on the IT landscape. Cyber insurance rarely reduces the overall risk, but merely distributes the costs. Despite the high return on investment in cybersecurity, developers often invest more in functional features than in security. However, only secure systems with a clear concept can guarantee resilience and data protection. In the private sector, too little is often invested in security measures because they are viewed purely as a cost factor. Since cybersecurity in shared infrastructure has the character of a public good – all users benefit, but hardly anyone has an individual incentive to invest alone – this suggests coordinated approaches that go beyond purely market-based mechanisms.

Many important OSS projects are developed by private individuals without sufficient security knowledge. Strategic professionalisation of processes through reviews, tests, and updates is necessary to ensure the security of this software. Code audits and DevSecOps tools are essential to minimise risks such as the Log4Shell vulnerability[78] in the widely used Java library Log4j, which compromised millions of systems worldwide in 2021 and highlighted the urgent need for action on the security of OSS dependencies. A study from Denmark[79] in 2025 shows that the Open Source Security Foundation (part of the Linux Foundation) and the Sovereign Tech Agency in Germany, as well as EU initiatives[80], are among the few working to finance security solutions, but government bureaucracy is slowing down necessary flexible market adjustments.

The dominance of American cloud providers also puts European infrastructure and data sovereignty at risk, as described above. Given the need for a crisis-resistant software landscape, it is necessary to build alternative infrastructures, as existing solutions often do not provide sufficient guarantees in terms of availability and confidentiality. As explained in section 3, OSS can play a central role.

[76] https://www.tagesschau.de/wirtschaft/unternehmen/jaguar-cyberangriff-100.html

[77] https://www.odni.gov/files/CTIIC/documents/products/Worldwide_Ransomware_2024.pdf

[78] https://en.wikipedia.org/wiki/Log4Shell

[79] https://arxiv.org/abs/2412.05887

[80] https://interoperable-europe.ec.europa.eu/sites/default/files/news/2022-04/Development%20of%20a%20Funding%20Mechanism%20for%20Sustaining%20Open%20Source%20Software%20for%20European%20Public%20Services.pdf

6 Conceptual proposal: Funding structures for a sustainable OSS ecosystem

This chapter outlines a reference model for support structures that professionalise and sustainably strengthen the existing OSS ecosystem. Although the following description is kept generic, it is necessary to develop customised funding structures for software products with specific requirements, such as in office automation or the ERP environment. Further down the software supply chain, however, ecosystems of different products may overlap, as they often use the same libraries and frameworks.

The core of the reference model is the establishment of a new type of organisation that – oriented toward market requirements and in the public interest – provides missing organisational building blocks and creates reliable guarantees for OSS. The creation of such an organisation stems from the requirement that long-term resilient software solutions should be operable without permanent ties to specific providers. This requires interchangeable components, migratable data formats, and open protocols. A central organisation can also effectively bridge the structural conflict of interest between competing corporate interests and collaborative software development.

The proposed reference model also pursues the following objectives:

Existence of software alternatives: Reduction of lock-in effects, flexibility in the operation of software components, and control over stored and processed data, insofar as this is legally compliant.

Interoperability and modularity: Interchangeability of infrastructure components due to open protocols, modularisation, and standardised interfaces.

Security and availability: Reduction of risks relating to failure, data leakage, and external manipulation of IT systems and technologies.

Digital sustainability: Maximisation of benefits for society.

6.1 Principles of the ecosystem

The OSS coordinator focuses on regulating software development and infrastructure operation and ideally follows the following principles:

Market viability and financing: The ecosystem must be self-sustaining in the long term, with financial incentives that ensure economically rewarding participation.

Openness and competition: Innovation cycles are accelerated and lock-in effects are reduced through interoperability and control over data.

Sustainable maintenance: The long-term maintenance of existing software – security updates, bug fixes, adaptation to new dependencies – is recognised as a standalone, fundable service and is systematically ensured. Maintenance must not be left to chance or the commitment of individual volunteers.

Complete transparency: All decisions, structures, and cash flows are clearly defined and transparent. Abuse is prevented through control by OSS communities and paying users.

Separation of development and operation: Decoupling development and operation responsibilities reduces dependence on a few software providers, as other participants provide services, creating the basis for a sovereign IT infrastructure.

Value through simplicity: Software use is simplified due to clarification of licensing and cost issues.

Community-driven prioritisation: How development goals are prioritised in the ecosystem has not yet been conclusively clarified. The OSS coordinator plays a central steering role, which inevitably raises the question of the extent to which the community and paying users actually have influence on decisions — and how conflicts of interest between these groups are resolved. It is also questionable whether a uniform prioritisation mechanism is suitable for all project types and sizes. These governance issues must be explicitly addressed as the funding structures are further developed.

Minimal administrative barriers: Enable easy entry, create incentives for participation, and allow flexible payment of financial compensation.

Service neutrality: Enable switching between service providers and software, similar to net neutrality.

Control over data: Solutions allow data extraction and migration. The separation of development and operation also enables the use of one's own infrastructure and full data control.

In order to achieve adequate financing, targeted support for smaller providers is advantageous, as they can often work in a more innovative and resource-efficient manner.[81]

Stable structures and comprehensive transparency are necessary to prevent commercial abuse of the funding structures; at the same time, decision-making processes must remain short in order to avoid excessive bureaucracy.

Political support is crucial in order to change the dependencies caused by market dynamics. Legal obligations and licensing costs are essential components of the ecosystem. In situations of crisis the openness of the source code of the underlying software components ensures that they still remain available. The goal is a self-sustaining ecosystem that – once it has reached a critical mass – offers measurable benefits to all participants, as is the case with the Linux kernel, for example. Support networks such as those around the kernel must be established and promoted in a targeted manner.

6.2 Design of the ecosystem

The proposed ecosystem includes the following stakeholders, in addition to customers and software users (left in fig. 3):

Open Source projects and developers (right): Responsible for the development and maintenance of OSS, supported by a constant and predictable flow of funds for planning and security vulnerability remediation as well as functional enhancements.

Operations (left): Responsible for operating and ensuring the availability and legal security of the software.

OSS Coordinator (center): Central organisation that provides the missing organisational components and guarantees, thereby bridging the conflict between competing companies and collaborative software development. It mediates the needs of providers, customers, and developers, structures OSS promotion, and is financed by feature requests.

Independent IT security auditors (top): Review the state of the software in the organisation and support the development of better security infrastructure.

External, non-profit funders (center bottom): Provide support, especially in traditionally financially weak areas such as networking and community building.

Specialised professionals (bottom left): Build a pool of skilled workers for technology and operational applications in companies.

[81] See the research corpus on the keyword *diseconomies of scale*.

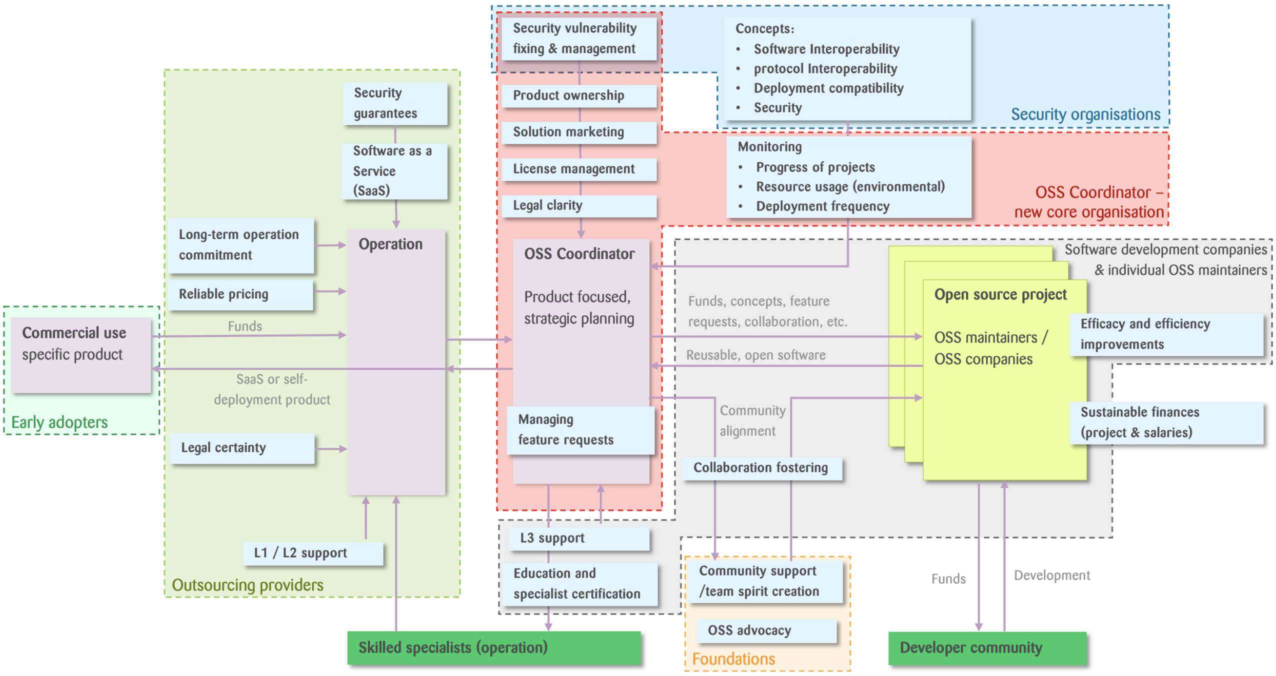
Security vulnerability fixing & management
Concepts:
Software Interoperability
protocol Interoperability
Deployment compatibility
Security
Security organisations
Product ownership
Solution marketing
License management
Legal clarity
Monitoring
Progress of projects
Resource usage (environmental)
Deployment frequency
OSS Coordinator – new core organisation
Security guarantees
Software as a Service (SaaS)
Long-term operation commitment
Operation
Reliable pricing
OSS Coordinator
Product focused, strategic planning
Software development companies & individual OSS maintainers
Commercial use specific product
Funds
Funds, concepts, feature requests, collaboration, etc.
Open source project
OSS maintainers / OSS companies
Efficacy and efficiency improvements
SaaS or self-deployment product
Reusable, open software
Early adopters
Community alignment
Managing feature requests
Sustainable finances (project & salaries)
Legal certainty
Collaboration fostering
L3 support
L1 / L2 support
Education and specialist certification
Community support /team spirit creation
Funds
Development
Outsourcing providers
OSS advocacy
Foundations
Skilled specialists (operation)
Developer community

Figure 3: Proposed ecosystem with cash and goods flows. This work focuses on the OSS coordinator at the center (in red), which, as the central organisation, provides the missing organisational components and guarantees, thereby bridging the conflict between competing companies and collaborative software development.

OSS communities (bottom right): The developer community is central, often organised on a voluntary basis, and should be explicitly promoted.

The funding structures should not replace OSS communities and developers, but rather provide targeted support — especially where the market currently lacks sufficient structures and incentives.

The OSS coordinator acts as a mediator between providers, customers, and OSS communities; covering tasks that go beyond actual software development. These include, in particular, the integration of suitable legal structures, the translation of market requirements into software functionalities, and the management of licenses. In addition, the OSS coordinator monitors the progress of projects, provides legal clarity, and coordinates training and the development of necessary technical skills.

Unless otherwise regulated, the OSS coordinator also ensures strategic oversight, coordination, and knowledge exchange with partner organisations and enables agile adjustments to user and developer needs, as described in the EuroStack Governance Framework[82]. Control and audit functions to ensure transparency and accountability are also an integral part of the OSS coordinator.

Another key task of the OSS coordinator is to provide and network skilled personnel who can develop and operate systems. Although qualified personnel are generally available, there is currently a lack of efficient structures for their coordinated cooperation and placement.

In addition, it may be useful to treat commercial and private uses differently in terms of licensing in order to protect the rights of developers while

[82] https://www.euro-stack.info/docs/EuroStack_2025.pdf

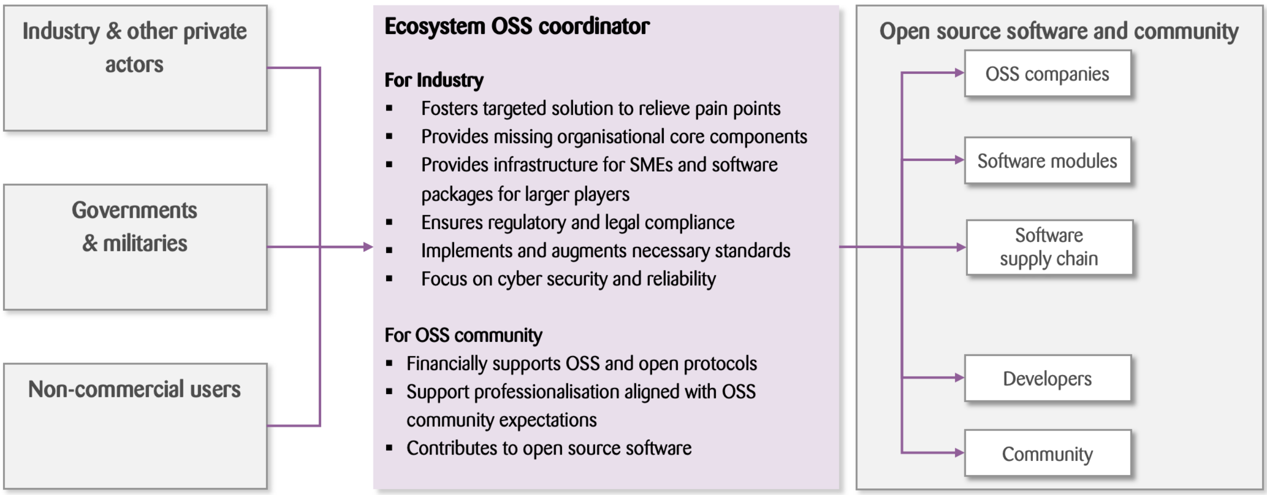
Industry & other private actors
Governments & militaries
Non-commercial users
Ecosystem OSS coordinator
For Industry
Fosters targeted solution to relieve pain points
Provides missing organisational core components
Provides infrastructure for SMEs and software packages for larger players
Ensures regulatory and legal compliance
Implements and augments necessary standards
Focus on cyber security and reliability
For OSS community
Financially supports OSS and open protocols
Support professionalisation aligned with OSS community expectations
Contributes to open source software
Open source software and community
OSS companies
Software modules
Software supply chain
Developers
Community

Figure 4: The OSS coordinator serves as a bridge between the different goals of the two worlds: the market (exclusion and control) and open source (collaboration).

promoting the distribution of the software. Such differentiation preserves the value of the software, enables low-threshold experimentation, and at the same time strengthens further development and innovation.

Appropriate incentive structures must be created to ensure that the ecosystem can function sustainably in a profit-oriented market. Financial resources should be directed to projects that have a significant impact on the software ecosystem, either through widespread use or through an integral role within the supply chain. The minimum requirement here is the sustainable maintenance of the software. Users should also be encouraged to use the ecosystem for accompanying services through appropriate licensing terms or concrete benefits.

In addition, funding for new technologies is required, which can be provided either through government programs or venture capital. Transparent and clearly traceable cash flows within the OSS coordinator are essential. Decisions on the use of funds and distribution criteria should be made jointly with the development community and users, supported by appropriate distribution metrics and partnerships (see section 4.2.2).

A flattening distribution curve of funds can contribute to the stability of the ecosystem: smaller projects are given greater consideration, while larger projects are given incentives to develop in a more modular way. This promotes competition, reusability, and innovation.

6.3 Role of cybersecurity

The cybersecurity community welcomes open structures, as security checks can be carried out more cost-effectively and easily in such environments, and vulnerabilities are often remedied more quickly thanks to collaborative processes. The two main areas of activity for relevant experts are, on the one hand, the improvement and automation of security checks during software development and, on the other hand, the external testing of finished solutions.

[83] https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

The impact of the EU Cyber Resilience Act[83] (CRA) on open source software is not yet fully clear[84]. However, the OSS coordinator can serve as a supporting structure by providing regulatory guidance and – where necessary – financial support for compliance and security efforts. The resulting lower security costs could particularly promote innovation in SMEs and start-ups.

These efforts are funded by the ecosystem and can be further strengthened by external funding sources such as foundations or government programs. While continuous process improvement is an integral part of effective cybersecurity, downstream testing should be considered a separate task and organised accordingly.

Testing is carried out in several steps: First, vulnerabilities must be systematically identified both within the software components of the ecosystem and in the underlying infrastructure. Next, coordinated remediation of the vulnerabilities must be ensured. This can be done, for example, by informing volunteer developers so that they can create the necessary patches. Alternatively, developers can be compensated for providing patches. Another option is to coordinate the remediation together with professional providers. In all cases, the process also includes monitoring progress and quality assurance of the submitted changes. Finally, coordinated prioritisation of the testing procedures is necessary to use resources effectively and efficiently.

It is essential that vulnerabilities are not only identified, but that their remediation is also sustainably integrated into the code base. This is made possible by the openness of the software and transparent access to the relevant artifacts and processes of software development, or through collaboration with companies that are already involved in the development of the component.

6.4 Role of philanthropy

Philanthropy can specifically promote activities that will be strategically relevant in the future or that, due to their nature, cannot be adequately financed through market mechanisms — in particular, community building and advocacy. An independent source of funding also strengthens the resilience of the OSS coordinator and can serve as a complementary mechanism for ensuring neutrality and control. Promising areas of application for philanthropic funds include:

- Initial start-up funding to strengthen and further develop the OSS ecosystem and coordinator
- Status reports on the current situation and on the bundling and overview of ongoing activities
- Potential analyses and convincing key figures and evidence for decision-makers
- Establishment, moderation, and strengthening of communities in prioritised solution areas
- Downstream measures such as independent testing, audits, and evaluations of the ecosystem and software (e.g. security testing)

6.5 Role of the state

Similar to philanthropy, the state can provide start-up financing to strengthen the OSS ecosystem. In addition, it can assume the following roles:

- Targeted promotion of relevant technologies and system architectures, including the development of corresponding expertise.
- Analysis of existing dependencies and assessment of the associated risks, as well as integration of the findings into funding measures.
- Linking public procurement and contracts to sovereignty and openness criteria in order to fund the ecosystem directly or indirectly.

[84] https://www.linuxfoundation.org/blog/understanding-the-cyber-resilience-act

- Establishing and maintaining international cooperation to develop sovereign and open solutions.
- Ensuring crisis response capability in the event of failures and threats, including the availability of sufficiently qualified specialists.

Government funding should support the open source ecosystem without replacing or controlling it. Companies and volunteers drive innovation, while government funding should ensure stability and security[85].

6.6 Role of the NTC

The NTC is involved in several ways: (a) as an independent testing organisation that tests developed software and actively supports the remediation of identified vulnerabilities, (b) as an interest group that brings cybersecurity issues into the Swiss political discourse, and (c) as a key partner that connects relevant decision-makers in Switzerland.

As part of this work, discussions have already been held on the potential of an open software infrastructure, which can be pursued by the NTC. The initial results of these discussions have been incorporated into this discussion paper.

7 Relevance of artificial intelligence

Advances in artificial intelligence are undeniably transforming the IT landscape in terms of software development[86] and security testing[87].

The automated generation of software is not a viable alternative to the use of freely available open source solutions. Even when using generative AI, sound technical expertise is required to ensure high-quality, maintainable, and secure software. In addition, the costs associated with individual development and maintenance, as well as the increased organisational effort, generally are higher than compared to collaboratively developed and maintained open source software.

While the effort required to fix and analyse security vulnerabilities is likely to decrease in the long term, the number and complexity of attacks are expected to increase. Thus, the urgency of the issues analysed in the discussion paper is likely to intensify in the medium-term.

Therefore, the following three-pronged approach should be considered: (a) The establishment of a dedicated research center to explore the possibilities for the beneficial use of AI to strengthen open source software and sovereign ecosystems. (b) Research into the application of AI in detecting vulnerabilities in code, both when pushing and in existing code, in order to counter potential attackers effectively and in a timely manner. (c) Further research initiatives to detect and remedy existing vulnerabilities through the use of AI technologies.

8 Recommendations

Based on the insights gained from this discussion paper, the following points are recommended in summary. The recommendations are primarily aimed at Swiss stakeholders, but some of them can only be effectively implemented in a European or international context — this should be taken into account when reading.

- Funding for follow-up work on this discussion paper, specifically a more detailed analysis of the practical market implications for OSS and the resulting target operating model for the proposed ecosystem.

[85] https://dri.es/funding-open-source-like-public-infrastructure

[86] https://www.cnbc.com/2025/04/29/satya-nadella-says-as-much-as-30percent-of-microsoft-code-is-written-by-ai.html

[87] https://aisle.com/blog/aisle-discovered-12-out-of-12-openssl-vulnerabilities

- Implementation of a small-scale pilot project as proof of concept to gather experience and establish a network.
- Investment in research into how the dynamics between open source software and the market for software products work today, how they can be shaped in the future, and how the balance can be struck. This includes, in particular, the analysis of incentive systems for a functioning ecosystem.
- Investment in the active development of cybersecurity capacity, including testing, to create and operate a sustainably stable IT infrastructure. Open system architectures should be considered to simplify implementation.
- Investment in research on the relationship between paid and volunteer labour within OSS projects. Introducing paid work into an existing volunteer community carries considerable risks: it can suppress intrinsic motivation, create imbalances and resentment, or shift the direction of development in favor of the paying parties — and thus cause lasting damage to the community that made the project possible in the first place. At the same time, financial incentives for professional maintenance are essential. How this tension can be constructively resolved is not yet sufficiently understood and must be explicitly addressed in the design of the OSS Coordinator.
- Investment in research on open licensing issues that the market cannot resolve on its own: in particular, on the legal compatibility of combining components under different licenses, on the empirical effectiveness of new hybrid models such as Fair Source or Fair Core, and on practical methods of license compliance for companies with many OSS dependencies.
- Identification and risk analysis of societally necessary IT infrastructure by government or government-affiliated organisations. This should be used to derive strategies for longer-term digital policy.
- General economic promotion of key technologies, products, and companies for open solutions. Creation of appropriate incentives and ecosystems. Promotion of skilled workers and their networking.

Although these recommendations are aimed at foundations, private-sector and government organisations, in the current political and economic climate, the initiative lies primarily with the government.

9 Next steps and outlook

The following steps should be taken on the path to a sustainably strengthened OSS ecosystem:

Detailed development of the OSS coordinator: The next step is to specify the target operating model, taking into account the relevant legal structures, governance, and administrative requirements. In addition, acceptance among the stakeholders involved must be ensured by conducting a cost-benefit analysis and establishing appropriate transparency mechanisms.

Development of a build-up strategy: In addition, basic funding must be secured and the first organisational steps and key milestones must be structured.

Building strategic partnerships: Furthermore, the integration of key partners from Switzerland, the EU, and the European environment must be ensured, involving actors from politics, business, and the OSS community.

A substantial improvement in the usability of open software is likely to significantly accelerate its spread and contribute to positioning in particular Switzerland as a technology center. Despite comparatively high labor costs, Switzerland could be an attractive location for the development and management of an OSS ecosystem due to less stringent regulation compared to the EU.

Authors

Dr. sc. ETH David M. Sommer: Cyber security expert at the innovation service provider Zühlke, product owner and tech lead, involved in the Digital Society Switzerland, subject matter expert at the University of Applied Sciences of Northwestern Switzerland in the Data Science program, organiser of multi-day events at the intersection of digitalisation and society.

Florian Kubiak: Theoretical physicist and programmer, specialised in numerical simulation and applied statistics, involved in social issues related to digital topics.

Dr. Raphael M. Reischuk: Co-founder and board member of the Swiss National Test Institute for Cybersecurity NTC, member of the Innovation Council of Innosuisse, member of the Cybersecurity Advisory Board of the Swiss Academy of Engineering Sciences SATW, and partner at the innovation service provider Zühlke.