A Balanced View of Open Source Software

Background

Open Source Software (OSS) and its socio-economic aspect has a role as a trigger for innovation, as a means to facilitate interoperability, and to set de-facto standards, as already described in the NESSI[1] position paper "Open Source Software" (2019)[2]. The recommendations and conclusions made in that paper are still valid: the European Commission should continue supporting the open source model as one way to facilitate easy access to fundamental technology under equal conditions to all organisations across Europe. But it should not preclude other models of software licensing (e.g. SaaS, proprietary), especially if this helps exploitation of research results. In particular, there should not be a general requirement that all the software developed in the context of a research project supported by public funding needs to be open source.

The European Commission has adopted an OSS strategy[3] and has published an OSS impact study[4].

- The strategy aims to "make the Commission part of the open source community", to co-develop with other European public-sector organisations, and to encourage the sharing and reuse of solutions, knowledge and expertise. The strategy considers OSS as a way to gain digital autonomy. Free access to source code allows developers to modify and customize the software as needed. Thus developers and users are not dependent on a specific software vendor, and avoid the risk that they do not have access to software and services due to some trade conflict.
- The study published by the Commission provides a detailed analysis of the positive impact that open source has on the European economy and recommends, among many other actions, "to provide strong incentives for uploading code generated in publicly supported R&D projects in publicly accessible EU-based OSSH (Open Source Software and Hardware) repositories." However, the study only considers negative aspects of OSS to a limited extent, discussing the role of large enterprises in OSS ecosystems and the potential downsides of sharing IPR from a geopolitical perspective, including the reduced option to impose sanctions or to control technology proliferation.

NESSI sees a strong need for a more balanced view on the advantages and the risks of OSS. The geopolitical tensions and the uncertainties related to cybersecurity, supply chains and markets have a greater impact on OSS ecosystems than outlined by the EC study, and therefore require more attention. For example, some popular open-source libraries have been corrupted by the maintainers of the OSS packages to protest the invasion of Ukraine and to sabotage software systems[5,6]. OSS security practices need urgently to be improved to cover these new threats, and geopolitical considerations must be taken into account when deciding whether or not to share results of European research as OSS.

[1] NESSI (Networked European Software and Services Initiative), the European association promoting research, development and innovation in the field of software, data and digital services; https://nessi.eu/
[2] https://nessi.eu/wp-content/uploads/2020/09/NESS-Open-Source-Software-issue1.pdf
[3] https://ec.europa.eu/info/departments/informatics/open-source-software-strategy_en
[4] https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and
[5] https://snyk.io/blog/peacenotwar-malicious-npm-node-ipc-package-vulnerability/
[6] https://www.bleepingcomputer.com/news/security/dev-corrupts-npm-libs-colors-and-faker-breaking-thousands-of-apps/

Elements of an OSS strategy

These issues point at the more general problem of finding a strategy which enables all the benefits of OSS whilst managing the risks associated with OSS. A recent report published by Boston Consulting Group[7] confirms the importance to have an OSS strategy in place that is based on a sound understanding of the merits and demerits of OSS.

NESSI considers the following to be particularly important elements of an OSS strategy:

- the governance and the health of the developer community behind an OSS project;
- the security of OSS; and
- the total cost of using OSS.

Open source communities

The use of OSS and the attempt to gain digital autonomy through OSS should help to avoid vendor lock-in. However, dependency on a specific software vendor is then replaced with dependency on the communities that are backing OSS projects and on any organisations that have a strong influence on these communities.

The health of these OSS communities is crucial for the quality and the reliable support of the software provided by OSS projects. What "healthy" means in this context is specified e.g. by the open source project CHAOSS[8]. The project develops metrics that assess the risks in OSS, help to understand the lifecycle and the value of an OSS project, and measure the diversity, equality and inclusion in OSS projects. It addresses questions such as who the contributors are and what their geographical location is, how much influence an organisation has on a community, how much time it takes to resolve defects and how well the code is tested, and how high the risk to a project is should the most active people leave.

These are all aspects that an OSS strategy of an organisation should consider when deciding about exploiting OSS or contributing to an OSS project. As already mentioned, geopolitical tensions might have an impact on OSS and the OSS supply chain, and may require greater attention in the OSS and OSS security context.

OSS security

The EC study concludes "that Open Source has cybersecurity-enhancing properties that if used correctly can make software more secure." This means that proper security and risk controls need to be in place and need to be used correctly in OSS projects, as it is the case for every software project There is significant need to improve in this area.

Like any other software, OSS includes vulnerabilities. Famous examples are Heartbleed[9] or more recently Log4j[10]. These incidents show that defects in small but widely used OSS libraries can cause systemic risks. A recent report[11] found that 29% of popular OSS projects contain at least one known security vulnerability. The same report points out that in 2021 software supply chain attacks have been increased by 650%. Such attacks do not exploit known vulnerabilities but implant malware directly into OSS projects and use the supply chain to propagate the malware and to compromise all software systems depending on those OSS projects.

It has been recognized that there is a need for action to address these risks. For example, the US Government has mandated organisations to create a Software Bill of Material (SBOM) to track direct, indirect and

[7] https://www.bcg.com/publications/2021/open-source-software-strategy-benefits
[8] https://chaoss.community/
[9] https://en.wikipedia.org/wiki/Heartbleed
[10] Log4j Vulnerability: What Security Leaders Need To Know and Do (gartner.com)
[11] https://www.sonatype.com/state-of-the-software-supply-chain/introduction

transitive dependencies of the software supply chain[12], and the Open Source Security Foundation (OpenSSF) has been formed to "address the urgent need for better security practices, tools and techniques in the open source software ecosystem."[13] Europe has taken action to ensure more secure software products by proposing the Cyber Resilience Act[14].

The cost of open source

As already outlined in the NESSI position paper "Open Source Software" (2019)[2], using OSS is not without cost. A decision to use OSS should be based on a sound understanding of the Total Cost of Ownership of OSS, including not only the direct initial costs on licenses and integration, but also all the indirect cost for operation, support, training, maintenance, handling of security incidents, contributing to OSS projects, etc.

OSS and European research projects

The EC study recommends providing strong incentives to publish the code that publicly supported R&D generates. NESSI believes that projects should be evaluated on a broad range of criteria which should not exclude business models other than OSS. Contributing to open source should not be a requirement in calls for proposals. Proposers and evaluators should consider the effects of open source R&D&I actions in the particular context of the proposal. This assessment should apply criteria such as those specified by CHAOSS[8], should learn the lessons from the many OSS initiatives which were not as successful as expected, and should recognise that both open and closed software approaches can generate economic and societal benefits including spillover effects.

Therefore, commercially successful European enterprises developing closed software should not be excluded from publicly supported research because of a general requirement to contribute to open source. Such a requirement would exclude some organisations from participating in those projects and thereby harm European players and the European economy.

Recommendations

NESSI recommends that the European Commission should:

- continue supporting the Open Source model as one way to facilitate easy access to fundamental technology under equal conditions to all organisations across Europe;
- not require that all software developed in the context of publicly supported projects should be open source; and
- take a balanced view on OSS, considering multiple aspects including the strategic value of the results of R&D&I activities.

[12] https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/
[13] https://resources.snyk.io/state-of-open-source-security-report-2022
[14] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act