

The Geopolitics of Code

From Digital Sovereignty to Global Fragmentation



[Talk at FOSDEM](#)

Daniel Izquierdo Cortázar,
Bitergia

Jesús M. González Barahona,
Universidad Rey Juan Carlos
@jqbarah@floss.social



Universidad
Rey Juan Carlos

FOSDEM, Brussels
February 1st, 2026

The Backstory

Can open source secure Europe's digital infrastructure?

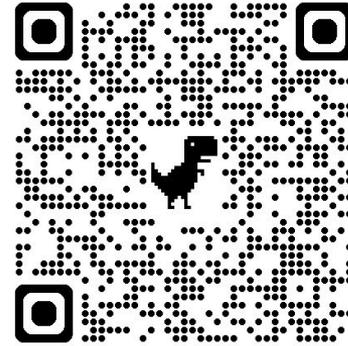


Darío García de Viedma



REAL INSTITUTO
elcano
ROYAL INSTITUTE

25
AÑOS · YEARS



[Can open source secure Europe's digital infrastructure?](#)





Global Challenges Require Global Collaboration

By Omar Mohsine, OSS Coordinator, United Nations

Since its founding, the United Nations has been built on a simple yet profound belief: *global challenges require global collaboration.*

The Charter of the United Nations recognizes that peace, prosperity, and human development cannot be achieved in isolation. No single country, institution, or organization—no matter how powerful—can solve the world's most pressing problems alone. From climate change to humanitarian crises, our progress has always depended on our ability to work together, share knowledge, and elevate collective wisdom over individual interest.

Today, this fundamental principle of collaboration extends beyond borders, cultures, and governments. It now lives and thrives in the digital world. Every day, millions of people—most of whom will never meet and may never even know



Why Do You Trust Software? I Don't.

By John Ellis, President & Head of Product, Codethink Ltd.

Software has become the critical infrastructure of the modern world, yet society continues to treat it as disposable. From hospitals and autonomous vehicles to financial markets and national grids, reliability has become assumed rather than engineered. The past two years, marked by the 2024 CrowdStrike outage, the 2025 Google Cloud failure, and continuing supply-chain breaches such as MOVEit and SolarWinds, exposed the limits of our current approaches to testing, certification, and assurance. Following, I argue that digital resilience will not emerge from compliance checklists but from measurable trust: transparent provenance,



<https://digitalresilienceforum.com/>



The Engine Room of Digital Sovereignty

By Adriana Groh, CEO, Sovereign Tech Agency

Resilience is not built in moments of calm. It takes crises for invisible systems to become visible—and for societies to remember that infrastructure is not simply what we build, but what we depend on every day. The pandemic, the war in Europe, and cascading software failures all pointed to the same structural fragility: our digital foundations were never designed to last.

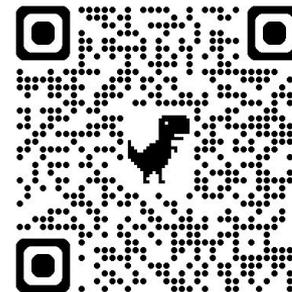
When I first spoke with the German government about the need to maintain open source, I did not need to convince them with abstract arguments about innovation. I only had to show them what breaks when infrastructure is neglected. Just as bridges collapse when maintenance is deferred,



Open Source not Local Source

By Amanda Brock, CEO, OpenUK

There's a profound misunderstanding across Europe around open source. I can live with people seeing what they want in this software: those on the left see it as socialist software, while libertarians believe it enables the free market through innovation and competition. In essence, open source democratizes tech, and makes the results available to everyone. However, I cannot live with the misguided thinking that lies behind the concept that open source is the "cornerstone of digital sovereignty." That's a juxtaposition.



Initial conclusions led to more...

- **...discussions**
- **...research**
- **...analysis**
- **...sharing with other stakeholders (here we are)**
- **...engaging again in further meetings**



Daniel Izquierdo Cortázar, PhD
CEO @ Bitergia & Co-Founder
Chair @ InnerSource Commons Foundation
Board Member @ CHAOSS



Jesus M. Gonzalez Barahona
Professor @ Universidad Rey Juan Carlos, Madrid
Bitergia Co-Founder

Context:

How FOSS Changed

Today's world

Octoverse Analysis 2025, GitHub

Tracking the top developer populations on GitHub (2020-2025)



	FIVE-YEAR TREND	2020 TO 2025 DEV COUNT	FIVE-YEAR CAGR*
1 United States	Steady #1	=10.2M to 28M	20.96%
2 India	+1 Spot	=4.5M to 21.9M	34.36%
3 China	-1 Spot	=6.1M to 10.7M	10.83%
4 Brazil	+1 Spot	=1.5M to 6.89M	33.27%
5 United Kingdom	-1 Spot	=1.7M to 4.8M	21.74%
6 Japan	+2 Spots	=1.2M to 4.5M	27.96%
7 Germany	-1 Spot	=1.4M to 4.4M	24.43%
8 Indonesia	+3 Spots	=0.9M to 4.37M	33.23%
9 Russia	-2 Spots	=1.4M to 4.16M	23.14%
10 Canada	-1 Spot	=1.2M to 3.46M	22.18%

Criterion	Max Mark	Bulgaria	France	Germany	Italy	Poland	Spain	United Kingdom	United States	Brazil	China	India	Japan	South Korea
Dimension: Public sector		52%	65%	0%	63%	2%	57%	51%	54%	14%	40%	40%	0%	31%
Policy existence	15	15	5	0	10	0	15	10	10	0	5	10	0	10
Public procurement	15	15	10	0	15	0	5	5	10	0	10	10	0	0
Policy implementation	15	3	8	0	4	0	5	6	6	0	5	5	0	0
OS competence	20	1	19	0	12	1	12	12	9	9	6	1	0	10
Dimension: Private sector		2%	29%	16%	13%	2%	20%	11%	0%	4%	56%	27%	7%	76%
Supporting private sector	20	0	0	2	0	1	0	0	0	0	14	5	1	17
Guidance	5	0	0	2	0	0	2	0	0	0	2	2	2	5
Community	10	1	10	1	4	0	6	3	0	1	4	4	0	6
OS present in neighbouring policies	10	0	3	2	2	0	1	2	0	1	5	1	0	6
Total of achievable mark		27%	47%	8%	38%	2%	38%	31%	27%	9%	48%	33%	3%	53%
Criterion	Max Mark	Bulgaria	France	Germany	Italy	Poland	Spain	United Kingdom	United States	Brazil	China	India	Japan	South Korea

Overview and comparison of Open Source policies

[The impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy](#) (European Commission)



**So, FOSS became
ubiquitous,
fundamental,
really global...**

**...maybe at the wrong
time in history**



How is FOSS affected?

- (Regulation)**
- (Choke Point)**
- (Weaponization)**

Linux Compliance with US Regulations



5. No Discrimination Against Persons or Groups

The license must not discriminate against any person or group of persons.

6. No Discrimination Against Fields of Endeavor

The license must not restrict anyone from making use of the program in a specific field of endeavor. For example, it may not restrict the program from being used in a business, or from being used for genetic research.

[...] If your company is on the U.S. OFAC SDN lists, subject to an OFAC sanctions program, or owned/controlled by a company on the list, our ability to collaborate with you will be subject to restrictions, and you cannot be in the MAINTAINERS file [...]

The screenshot shows a web browser window with the URL `lwn.net/Articles/995186/`. The page header includes the LWN.net logo, navigation links for 'Content' and 'Edition', and user options for 'Log in / Subscribe / Register'. The main heading of the article is 'Several Russian developers lose kernel maintainership status', with a sub-header indicating it was posted on October 22, 2024 by corbet. The article text begins with: 'Perhaps one of the more surprising changes in the 6.12-rc4 development kernel was the removal of several entries from the kernel's MAINTAINERS file. The patch performing the removal was sent (by Greg Kroah-Hartman) only to the patches@lists.linux.dev mailing list; the change was included in a char-misc drivers pull request with no particular mention.'

```
From: quake <quake.wang@gmail.com>
To: linux-kernel@vger.kernel.org
Cc: Quake Wang <quake.wang@gmail.com>
Subject: [PATCH] Remove Huawei
Date: Thu, 24 Oct 2024 12:26:37 +0900 [thread overview]
Message-ID: <20241024032637.34286-1-quake.wang@gmail.com> (raw)
```

```
From: Quake Wang <quake.wang@gmail.com>
```

```
Remove some entries due to various compliance requirements. They
cannot come back in the future as huawei is sanctioned by most freedom
countries in the world.
```

CRA effect on OSS Developers



Shaping Europe's digital future

[Home](#) | [Policies](#) | [Activities](#) | [News](#) | [Library](#) | [Funding](#) | [Calendar](#) | [Consultations](#) | [AI Office](#)

[Home](#) > [Policies](#) > [Cybersecurity](#) > [EU cybersecurity policies](#) > [Cyber Resilience Act](#) > [Cyber Resilience Act - Open source](#)

Cyber Resilience Act - Open source

The Cyber Resilience Act has a special approach to free and open-source software, given its central role in ensuring the cybersecurity products with digital elements and its contributions to the European Union's economy.

How does the CRA address free and open-source software?

<https://digital-strategy.ec.europa.eu/en/policies/cra-open-source>



By David A. Wheeler

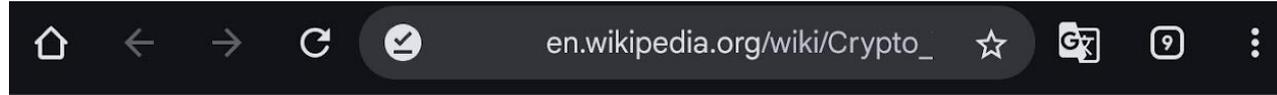
Software is about to be regulated worldwide. Are you ready?

Specialized software, such as software in medical devices, has been regulated for years. But laws on specialized software affected very few developers. The European Union (EU) [Cyber Resilience Act \(CRA\)](#) is fundamentally different. It's a law that applies to software, hardware, products containing them, and their backend services, if [made available](#) on the European market. The law applies regardless of where its developers are located. While technically the CRA isn't a worldwide law, in practice it's worldwide, because software is often distributed and used globally. What's more, failing to comply with the CRA where required can lead to not only a stop in sales, but also steep penalties (up to €15M or 2.5% worldwide annual turnover whichever is greater), and its obligations begin on 2026-09-11.

<https://openssf.org/blog/2025/07/15/new-cyber-resilience-act-cra-brief-guide-for-oss-developers/>

Crypto Wars

Regulation
affecting FOSS
is not
something new



Crypto Wars

🌐 9 languages ▾

Article [Talk](#)

Read [Edit](#) [View history](#) [Tools](#) ▾

From Wikipedia, the free encyclopedia

The controversy unofficially dubbed the "**Crypto Wars**" involves attempts by the [United States](#) (US) and allied governments to limit access to [cryptography](#) strong enough to thwart [decryption](#) by national intelligence agencies, especially the [National Security Agency](#) (NSA), and the response to protect [digital rights](#) by privacy advocates and civil libertarians.^{[1][2]}

[Export of cryptography from the United States](#) [\[edit\]](#)

Main article: [Export of cryptography from the United States](#)

[Cold War era](#) [\[edit\]](#)

GitHub Sanctions

What happens when
developers are banned in
software development
platforms?

(“when”, no longer “if”)

arXiv > cs > arXiv:2404.05489

Computer Science > Software Engineering

[Submitted on 8 Apr 2024]

The Impact of Sanctions on GitHub Developers and Activities

Yumei Fan, Ani Hovhannisyan, Hideaki Hata, Christoph Treude, Raula Gaikovina Kula

The GitHub platform has fueled the creation of truly global software, enabling contributions from developers across various geographical regions of the world. As software becomes more entwined with global politics and social regulations, it becomes similarly subject to government sanctions. In 2019, GitHub restricted access to certain services for users in specific locations but rolled back these restrictions for some communities (e.g., the Iranian community) in 2021. We conducted a large-scale empirical study, collecting approximately 156 thousand user profiles and their 41 million activity points from 2008 to 2022, to understand the response of developers. Our results indicate that many of these targeted developers were able to navigate through the sanctions. Furthermore, once these sanctions were lifted, these developers opted to return to GitHub instead of withdrawing their contributions to the platform. The study indicates that platforms like GitHub play key roles in sustaining global contributions to Open Source Software.

<https://arxiv.org/abs/2404.05489>



The XZ-utils backdoor

Re: [xz-devel] XZ for Java

Lasse Collin | Wed, 08 Jun 2022 03:28:08 -0700

On 2022-06-07 Jigar Kumar wrote:

```
> Progress will not happen until there is new maintainer. XZ for C has
> sparse commit log too. Dennis you are better off waiting until new
> maintainer happens or fork yourself. Submitting patches here has no
> purpose these days. The current maintainer lost interest or doesn't
> care to maintain anymore. It is sad to see for a repo like this.
```

I haven't lost interest but my ability to care has been fairly limited, mostly due to longterm mental health issues but also due to some other things. Recently I've worked off-list a bit with Jia Tan on XZ Utils, perhaps he will have a bigger role in the future, we'll see.

It's also good to keep in mind that this is an unpaid hobby project.

Anyway, I assure you that I know far too well about the problem that not much progress has been made. The thought of finding new maintainers has existed for a long time too as the current situation is obviously bad and sad for the project.

A Deep Dive on the xz Compromise

April 2, 2024 - 14 min



Author:

Joao Correia

Technical Evangelist

CVE-2024-3094 XZ Backdoor: All you need to know



By Shachar Menashe, JFrog VP Security Research | Jonathan Sar Shalom, JFrog Director of Threat Research | Brian

Moussalli, JFrog Malware Research Team Leader | March 31, 2024

<https://www.mail-archive.com/xz-devel@tukaani.org/msg00567.html>

<https://tuxcare.com/blog/xz-compromise/>

<https://jfrog.com/blog/xz-backdoor-attack-cve-2024-3094-all-you-need-to-know/>

A Linux backdoor attempt... back in 2003

The Register®

This article is more than 1 year old

Linux kernel backdoor blocked

Hints at smarter hacks

 [Kevin Poulsen](#)

Fri 7 Nov 2003 // 13:06

Software developers on Wednesday detected and thwarted a hacker's scheme to submerge a slick backdoor in the next version of the Linux kernel, but security experts say the abortive caper proves that extremely subtle source code tampering is more than just the stuff of paranoid speculation.

The Linux Backdoor Attempt of 2003

October 9, 2013 - by [Ed Felten](#)

[Comments](#)

 Privacy & Security

Josh [wrote](#) recently about a serious security bug that appeared in Debian Linux back in 2006, and whether it was really a backdoor inserted by the NSA. (He concluded that it probably was not.)

Today I want to write about another [incident](#), in 2003, in which someone tried to backdoor the Linux kernel. This one was definitely an attempt to insert a backdoor. But we don't know who it was that made the attempt—and we probably never will.

<https://blog.citp.princeton.edu/2013/10/09/the-linux-backdoor-attempt-of-2003/>
https://www.theregister.com/2003/11/07/linux_kernel_backdoor_blocked/

**These issues aren't new,
but they're becoming more frequent and concerning
due to FOSS relevance and the geopolitical context**

FOSS becoming a target

FOSS becoming a weapon

The Reality of the Industry, an example

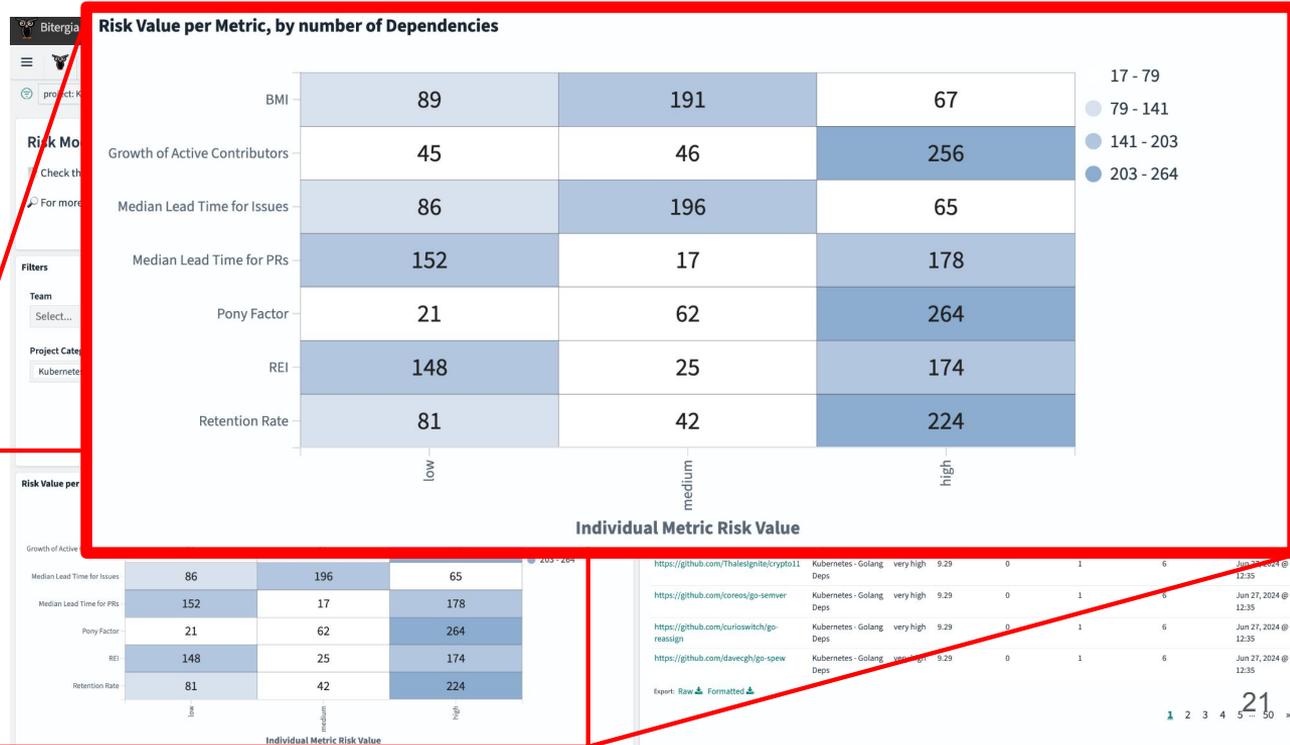
Bitergia Research

First level dependencies of Kubernetes, only Go programming language.

~ 400 packages

2/3 are at high risk of becoming unmaintained

(bus factor, talent retention, no contributors growth)



Strategies



The USA way

- Main FOSS Foundations under USA jurisdiction
- Huge private and public funding
- Clear involvement of many tech companies
- Control of basic infrastructure (such as GitHub)

De facto control of many FOSS projects under US rules.

The Chinese way

- Important role of the government (funding, strategy)
- More and more focus on creating their own FOSS stacks
- Organizing around China-based foundations (OpenAtom)

The lack of open governance might be seen as a threat

The European way

???

Now that FOSS is becoming truly global

(perhaps at the worst time in recent history to be global)

and is truly essential...

(when any essential asset is weaponized)

**...can FOSS survive
as a worldwide community?**

Detour: **An analogy**



Paths

We have built paths since we're humans (and earlier)

First, just by walking

Then, by constructing, improving them

In a fully decentralized, loosely coordinated way



Problems

There are dragons out there
(thieves, warlords, ...)

Lack of coordination means lack
of efficiency

Local and regional regulations
apply and make travel difficult

Many gaps, no one is really in
charge of maintaining routes

Solutions

Paths as infrastructure

Improvements on funding,
coordination

Legal framework

Services (security, food,
accommodation) to increase
their usefulness

Basic facility for our world

The Roman world already
understood this

**An alternative
option:
FOSS as shared
infrastructure**



What?

FOSS as a foundation of our society

Essential infrastructure, like roads, railways, electric grids, communication networks, public libraries

Many kinds of benefits:

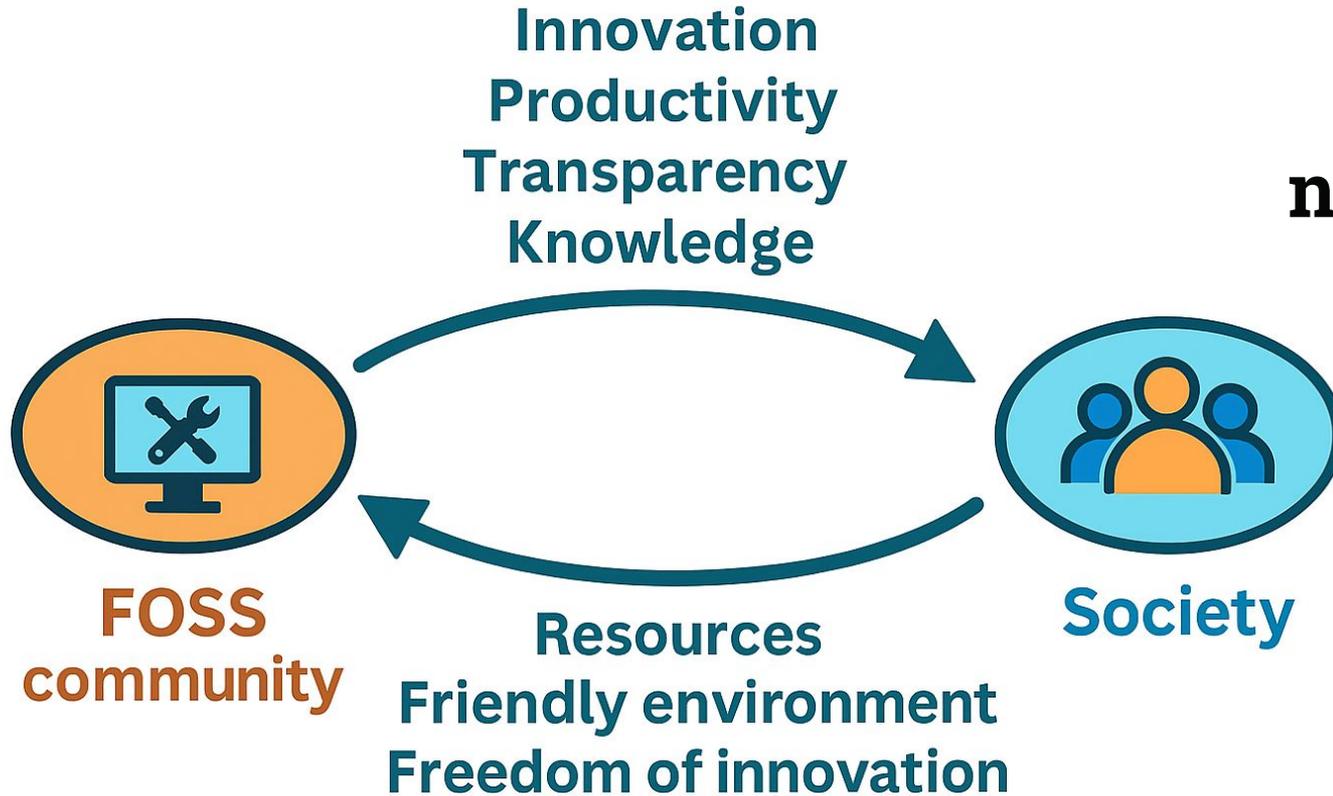
- Innovation: lowers barriers
- Transparency: can be inspected
- Productivity: focus on the added value
- Knowledge transfer: encoded in the software
- ...

FOSS is a common good

Positive feedback loop by

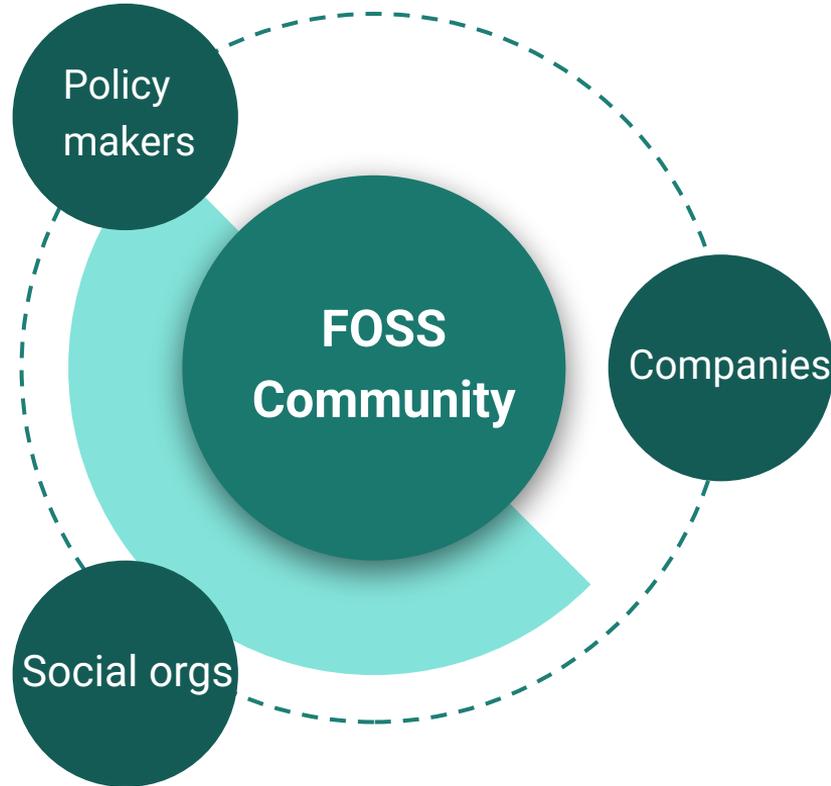
nurturing,

not controlling



Who?

We're the people who can (should?) explain this



How?

Change scale.

Involve all actors willing to join

Coordinate.

Worldwide.



Support

Promote FOSS-based
services and apps

Ensure a FOSS-friendly
Environment

Remove barriers
for FOSS

Fill the gaps

Don't interfere

Let FOSS projects
make their decisions

Let users / industry
decide which FOSS to use

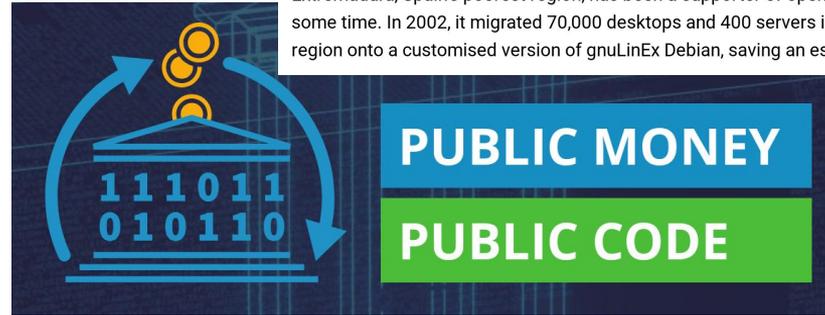
Let cooperation combine
with competition

Promote: Some examples

Preference for FOSS in public procurement

All software funded with public money licensed FOSS

Fund FOSS components for open standards



Art. 16 da [Lei nº 14.063, de 23/09/2021](#):
estabelece que os sistemas de informação e de comunicação desenvolvidos exclusivamente pela administração pública são regidos por licença de código aberto, permitida a sua utilização, cópia, alteração e distribuição sem restrições por todos os órgãos e entidades públicos.

Extremadura.gov switches onto Linux

Software libre for Spanish junta

John Leyden

Wed 2 Aug 2006 13:12 UTC

The Spanish region of Extremadura has pledged to move all government computers onto open source software within the next year. Officials will be mandated to use the open document format standard for office communications over the same time frame.

Extremadura, Spain's poorest region, has been a supporter of open source software for some time. In 2002, it migrated 70,000 desktops and 400 servers in schools across the region onto a customised version of gnuLinEx Debian, saving an estimated €18m.

NGI Zero grant programmes

The current grant programmes run by NGI Zero are:

- [NGIO Commons Fund](#)

public nature of the internet
medium-sized R&D grants between 5,000 and 50,000 euro, ability to scale up. Available to both individuals and organisational type. You can apply at any time in the rolling open calls that take place every two months.

architecture of the Internet and openness of technology forward
grant programme available to both individuals and organisations of any type. The proposal call has closed but development of funded projects is ongoing. Check out the [ongoing](#) projects funded by NGIO Core.



FOSS-friendly: Some examples

**Fostering open source
across countries**

**Open source as the basic
fundamental blocks for
technology**

**The UN Open Source
Principles**



**United
Nations**

Office for Digital and Emerging Technologies



Home » Ongoing Work » Digital Public Goods



Promoting open-source solutions for a more equitable world

FOSS-friendly: Some examples

Ensure that regulation does not harm FOSS

Clarify legal protections to FOSS developers

Clear difference between "producing and testing FOSS" and "using FOSS in production" (liability, etc.)



Shaping Europe's digital future

< [Cyber Resilience Act](#)

Cyber Resilience Act - Open source

BRIEFING

EU Legislation in Progress



European Parliament

Revised Product Liability Directive

Remove barriers: Some examples

Certification procedures allowing FOSS

Remove requirements mandating proprietary formats, technologies

Ensure proper understanding of the use of FOSS

Be open and use open source

Publish your code and use open source to improve transparency, flexibility and accountability.

From: [Government Digital Service](#) and [Central Digital and Data Office](#)

Published 6 November 2017

Last updated 31 March 2021 — [See all updates](#)

Eclipse Safe Open Vehicle Core

[Overview](#)

[Downloads](#)

[Who's Involved](#)

[Developer Resources](#)

[Governance](#)

[Contact Us](#)

The Eclipse *Safe Open Vehicle Core* project aims to develop an open-source core stack for Software Defined Vehicles (SDVs), specifically targeting embedded high-performance Electronic Control Units (ECUs).

As these ECUs carry multiple processors, the project also targets for interoperability between these processors.

To ensure applicability in the automotive domain we ensure compliance with relevant safety standards, such as ISO 26262 for functional safety, providing a reliable foundation for safety-critical applications and adherence to stringent security standards, implementing robust cybersecurity measures in accordance with ISO/SAE 21434 and UNECE WP.29.

Fill the gaps: Some examples

Support critical, underresourced projects



FLOSS/fund

\$1 million a year for free and open source projects

For individuals and orgs, big and small.

 open collective

Solutions ▾ Product ▾ Organization ▾ 🔍 Search

Sign Up

Help to improve quality of popular FOSS products

Support critical infrastructure



With the Sovereign Tech Fund, we invest globally in the open software components that underpin Germany's and Europe's competitiveness and ability to innovate. By targeting core digital infrastructure, our investments

The future is collective

We make it easy to **raise, manage, and disburse money with full transparency**. Start your open collective, apply to a Fiscal Host, and unlock funding for your community—free from red tape.

Combination and coordination

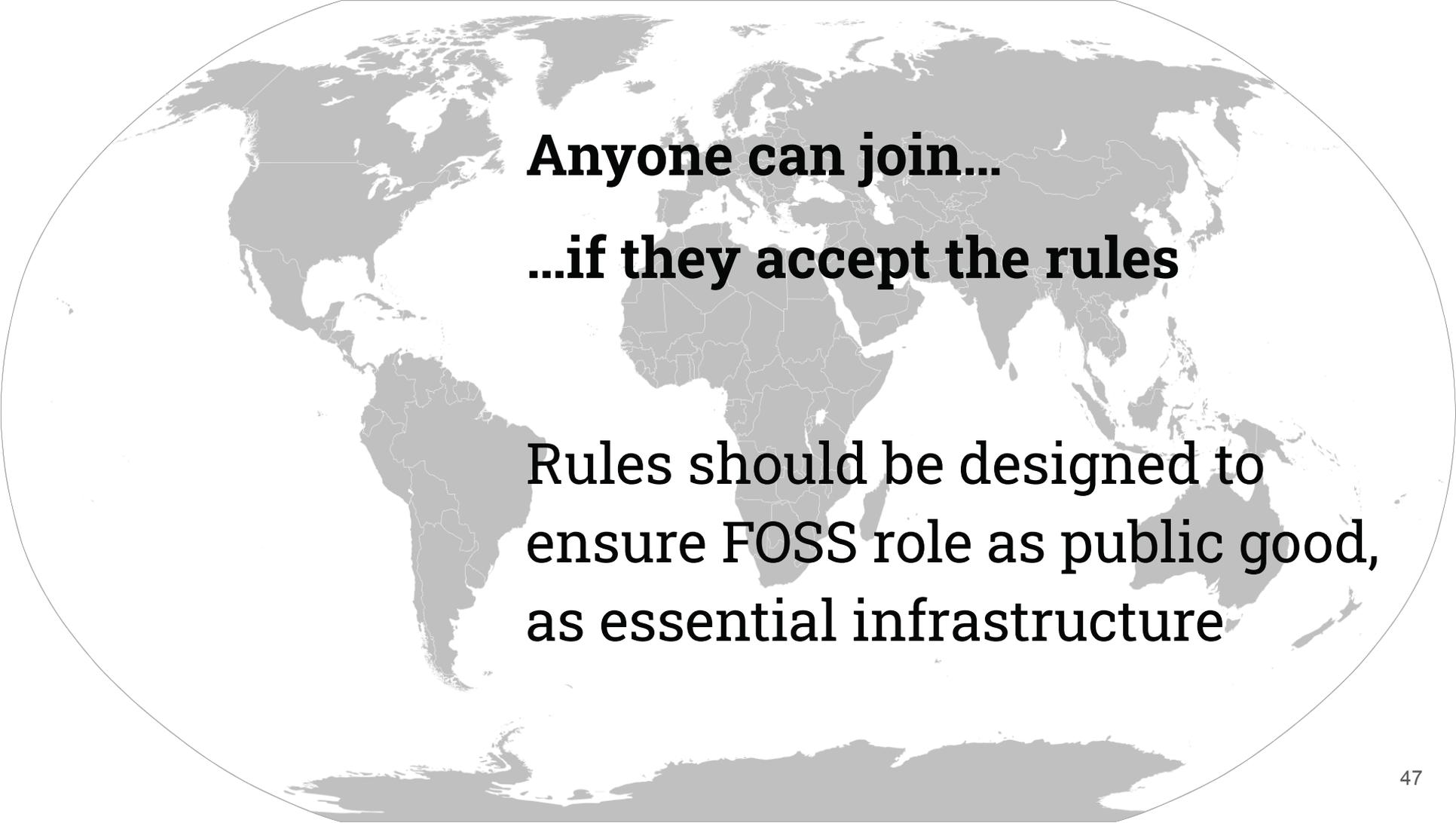
Governments

**FOSS
Projects**

Foundations

Companies

Where?



Anyone can join...

...if they accept the rules

Rules should be designed to
ensure FOSS role as public good,
as essential infrastructure

Why?

Those joining will benefit
Those not joining risk being left behind

This is not a zero-sum game:
there is a lot to benefit from collaborating
(while still competing)

Problems to solve

Weaponization

Lack of investment

Fragmentation

And still...

- How to help projects to improve (the one-million-euro challenge)
- How to ensure innovation is favored, not driven (it is difficult to drive innovation better than innovators themselves)
- How to ensure incentives to keep resource flowing towards developers
- How to ensure competition is not biased, making it less efficient
- How to still promote collaboration

And many, many more issues to solve

We need...

- **more experience**
- **more experiments**
- **more research**



**Is Europe
ready to
lead?**

And / or collaborate with others?



China's Open-Source Strategy: Innovation, Sovereignty, and Global Risk



DOUG LEVIN
SEP 16, 2025



Share

Yesterday's *Lessons* post analyzed the AI strategies of China and the United States, concluding they diverge sharply, each shaped by its governance model and priorities. [\[Here\]](#) That discussion raised questions among readers about China's open-source strategy—questions this post now explores.



Growing India's FOSS Ecosystem

Just some examples...



...or miss this train?

Free Software / Open Source: Information Society Opportunities for Europe?

Working group on Libre Software¹

December 1999
Version 1.0a

Abstract

Open source software is becoming the most interesting ‘new’ phenomenon of the entire information technology landscape, generating a level of interest similar to that of the first moments of the Internet. However, as we will show in this document, the open source software phenomenon is not historically new, although in recent years it has reached a critical mass, which has allowed it to enter the mainstream software market.

The impact of open source technology is expected to be quite noticeable in the software industry, and in society as a whole. It allows for novel development models, which have already been demonstrated to be especially well suited to efficiently take advantage of the work of developers spread across all corners of the planet. It also enables completely new business models, which are shaping a network of groups and companies based on open source software development. And it has, in general, a very positive impact as an enabler for the creation of new markets and business opportunities.

Despite these facts, many people think that the open source movement is merely another temporary fashion in the software industry. On the contrary, many other believe that changes caused by open source will be so deep that they will completely shape the software industry of the first decade of the 21st century. This document tries to provide some facts, opinions, and references, so that the reader can decide if all of this is just nonsense, or if it deserves more and better study and consideration.

<https://hdl.handle.net/10115/155697>

**The question is not if we can do it.
We have the talent, the resources,
and know-how.**

**The question is:
Do we believe FOSS drives
innovation and better digital services?
And Europe is a good home for FOSS?**

Hot off the press!!



European Commission Call for Evidence

European Open Digital Ecosystems

[Have your say - Public Consultations and Feedback](#) > [Published initiatives](#) > [European Open Digital Ecosystems](#)

In preparation

Call for evidence

Feedback period

06 January 2026 - 03

February 2026

Feedback: Open

About this initiative

Summary

The European Open Digital Ecosystem Strategy will set out:

- a strategic approach to the open source sector in the EU that addresses the importance of open source as a crucial contribution to EU technological sovereignty, security and competitiveness
- a strategic and operational framework to strengthen the use, development and reuse of open digital assets within the Commission, building on the results achieved under the 2020-2023 Commission Open Source Software Strategy.

Again:

**Likely everyone here will agree with
FOSS delivering innovation and other benefits,
but**

Do we really believe it?

The Geopolitics of Source Code

Daniel Izquierdo, Bitergia

Jesús M. González Barahona, Universidad Rey Juan Carlos

References

[Funding Open Source like public infrastructure](#) by Dries Buytaert

[Can open source secure Europe's digital infrastructure?](#) by Darío García de Viedma

[World of open source: Europe spotlight 2022](#) by Colin Eberhardt, Graham Odds, Matthew Dunderdale, Scott Logic

[The innovations of open source](#) by Dirk Riehle

[The impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy](#)
(European Commission)

[Free Software / Open Source: Information Society Opportunities for Europe?](#) (1999)

Credits & License

Website screenshots included under the right of quotation

“English riots in the Iranian press in Tehran”, by Kai Hendry, CC BY 2.0,
<https://commons.wikimedia.org/w/index.php?curid=19959384>

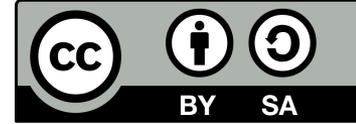


The Blue Marble, by NASA, Public Domain
<https://commons.wikimedia.org/w/index.php?curid=10548723>



Réserve naturelle nationale de la baie de Somme, CC BY-SA 4.0
<https://commons.wikimedia.org/w/index.php?curid=79252016>





Copyright 2026 Daniel Izquierdo, Jesus M. Gonzalez-Barahona
Some rights reserved

This document is distributed under the Creative Commons
Attribution-ShareAlike 4.0 International
except for figures where other license is stated

<https://creativecommons.org/licenses/by-sa/4.0/>

The Geopolitics of Source Code

Daniel Izquierdo Cortázar,
Bitergia



Jesús M. González Barahona,
Universidad Rey Juan Carlos
[@jqbarah@floss.social](mailto:jqbarah@floss.social)



Universidad
Rey Juan Carlos

FOSDEM, Brussels
February 1st, 2026

Open source represents 70% to 90% of modern software codebases and this is today seen as as a crucial global public infrastructure by many players. Given its ubiquity, this is increasingly part of geopolitical discussions and national-security agendas. This presentation will analyze the risks and governance challenges at the intersection of open source and global politics, with a focus on the recent European discourse on digital sovereignty and supply-chain security.

The core dilemma is that open source's power lies in the mutualization of risk (collective maintenance and faster vulnerability detection), but this is being undermined by fragmentation along national and corporate lines. We will explore:

The Weaponization of Open Source: How jurisdictional control over key platforms (like GitHub and PyPI, largely hosted by US entities) translates into geopolitical tools (the "Panopticon" and "Chokepoint" effects), as seen in the 2019 GitHub sanctions.

Lack of Investment: The crisis of critical components being maintained by small, under-resourced teams, creating an ecosystem that powers the global economy but lacks the resources to secure itself (e.g., the Log4j incident, XZ, and others).

The Fragmentation Trend: The response from nations like China, which are building domestic repositories (Gitee, OpenAtom Foundation) as part of a plan for technological self-sufficiency. This fragmentation reduces interoperability and shared visibility. This makes open source more weak and less resilient.

The presentation will conclude by openly discussing a shared call to action for the FOSS community: How can we forge a stronger shared responsibility between developers, policymakers, and industry to mitigate these losses and keep open source secure, interoperable, and globally accessible?.