Assessing the Lack of Digital Sovereignity in Critical Open Source Components

Jean Leneutre, **Stefano Zacchiroli**

Télécom Paris
stefano.zacchiroli@telecom-paris.fr

7 Dec 2021
COPIL Chaire Cyber et Souveraineté Numerique
Institut des Hautes Études de Défense Nationale (IHEDN)

About the speaker

- Professor of Computer Science, Télécom Paris, Institut Polytechnique de Paris
- Free/Open Source Software activist (20+ years)
- Debian Developer & Former 3x Debian Project Leader
- Former Open Source Initiative (OSI) director
- Software Heritage co-founder & CTO

Context — Free/Open Source Software is Everywhere

- Modern software development relies heavily on software reuse
- Specifically, reuse of Free / Open Source Software (FOSS)
  - 96% of software products on the market contains at least *some* open source code in them (OSSRA 2020, Synopsis)

This induces dependencies of different kinds:

1. Development *processes and tools* — e.g., GitHub, Travis, VS Code
2. Specific *open source components* — popular languages, libraries, frameworks, etc.

- What happens to our development activities if we lose access to dependencies?
- Who can affect our software development practices via dependencies?
- Such actors can sneak code into our products and impact us via technical decisions

Digital Sovereignty Implications

As part of this action we propose to perform a digital sovereignty assessment exercise about critical open source components that will answer the following questions.

- Who develops critical FOSS components we depend upon for sw. development?
- Which type of actors are them?
  - individuals / public bodies / for-profit companies / non-profit organizations
- Where, and in particular in which countries, are those actors based?
- What would be the impact of losing access, temporarily or in the long run, to the relevant software components
  - e.g., due to *unavailability* or changes in *intellectual property* regimes?
- Which preemptive countermeasures can be put in place to mitigate the impact of losing that access?

Action Description

- Identify use cases based on *chaire* partners interests: full ecosystems (e.g., Python, Node, Java, etc.) and/or development practices and tools
- Define a methodology that, given as input a (potentially large) set of FOSS projects, produces as output an overview of who contributes to them
- For each use case, identify critical dependencies on 3rd-party FOSS components
- For each identified dependency, determine the practical and business impact of losing access to it
- For each identified dependency, determine who develop it and collect all relevant data that could inform strategic decisions (type of actor, geographic location, business model and funding, etc.)
- Summarize findings in a comprehensive report
- Recommend digital countermeasures to either eliminate dependencies or mitigate the impact of losing access to them

Project Management Details

Timeline

T+0M	kick-off
T+2M	use cases identification
T+8M	analysis of technical dependencies
T+10M	analysis of relevant geopolitical data
T+12M	summary of findings and recommendations (report)

Wrapping Up

- FOSS components are commonplace critical dependencies in software development and that has profound implications on our digital sovereignty
- We will explore who develop critical FOSS components we depend upon and characterize them along geopolitical aspects like geographical origin and actor type
- We will summarize our findings and propose risk mitigation approaches

Contacts

Stefano Zacchiroli / stefano.zacchiroli@telecom-paris.fr