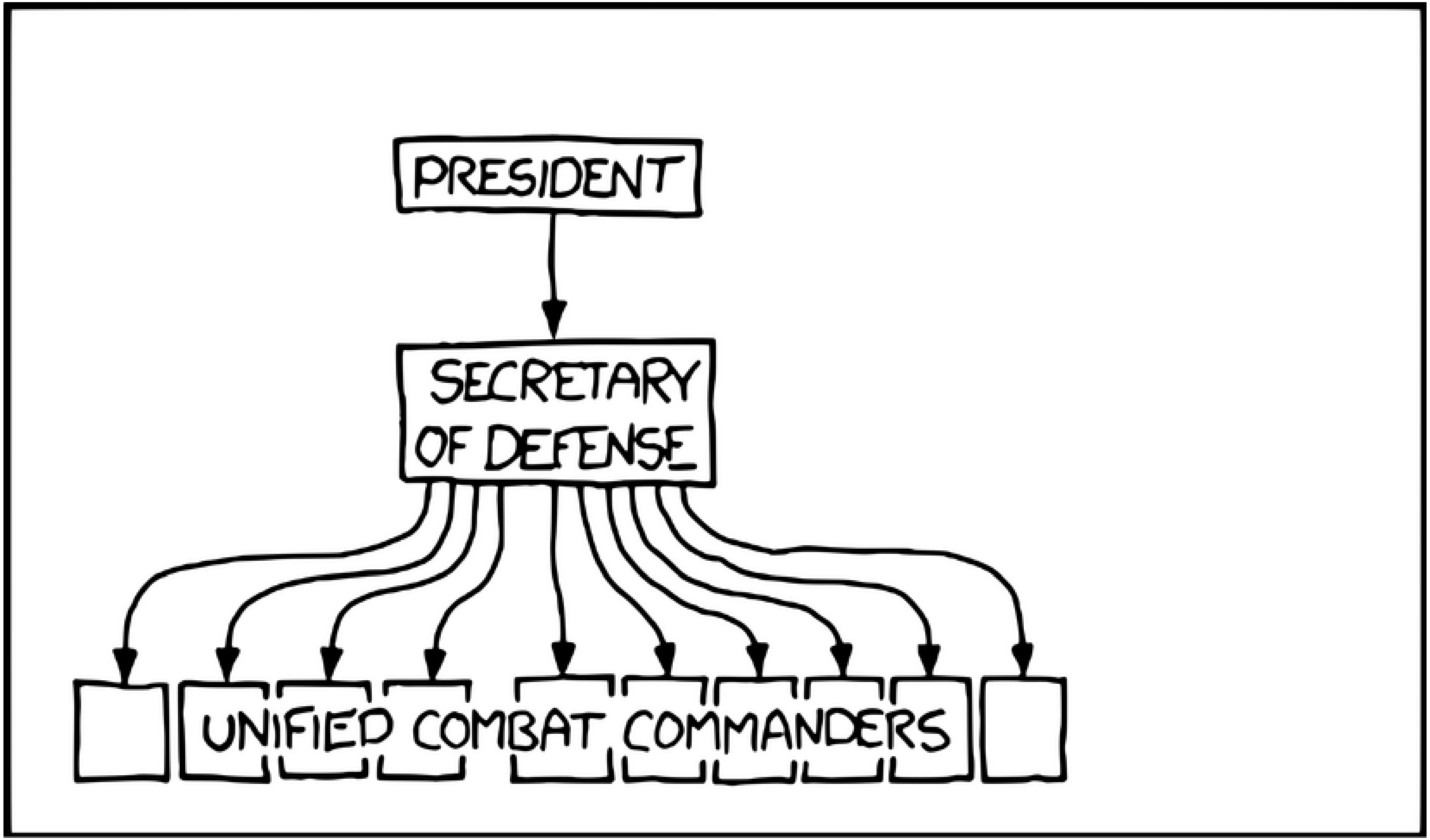
No IT Security without Free Software

How Openness Contributes to IT Security

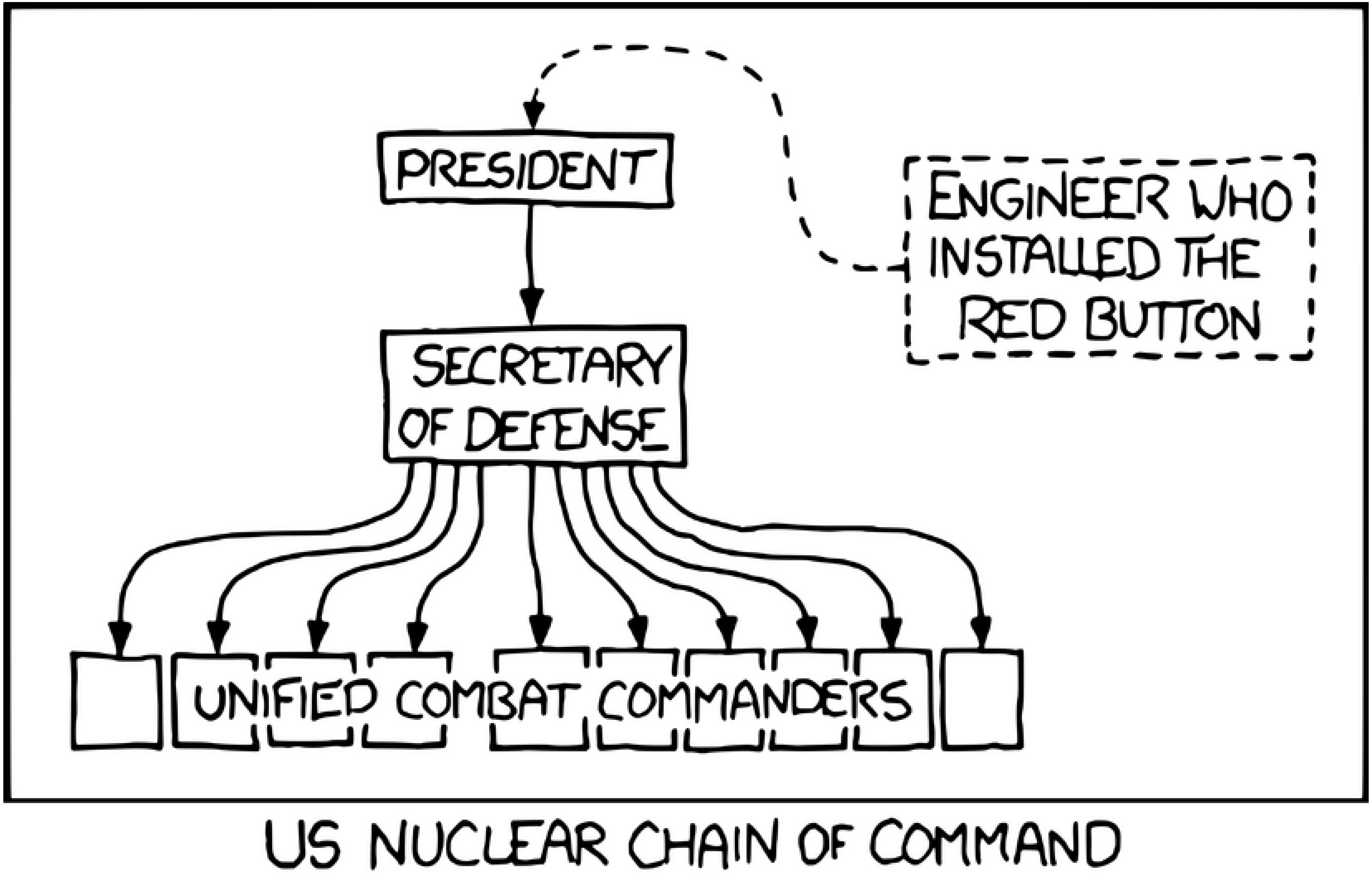
20 November 2020 · DeepSec

Max Mehl · Program Manager · fsfe.org/about/mehl · @mxmehl

A charity that empowers users to control technology



US NUCLEAR CHAIN OF COMMAND


PRESIDENT
SECRETARY OF DEFENSE
ENGINEER WHO INSTALLED THE RED BUTTON
UNIFIED COMBAT COMMANDERS
US NUCLEAR CHAIN OF COMMAND

Free Software

Use

Software can be used for any purpose, without restrictions

Study

Software can be analysed by everyone. The source code is available

Share

Software can be shared freely with anyone, without limitations

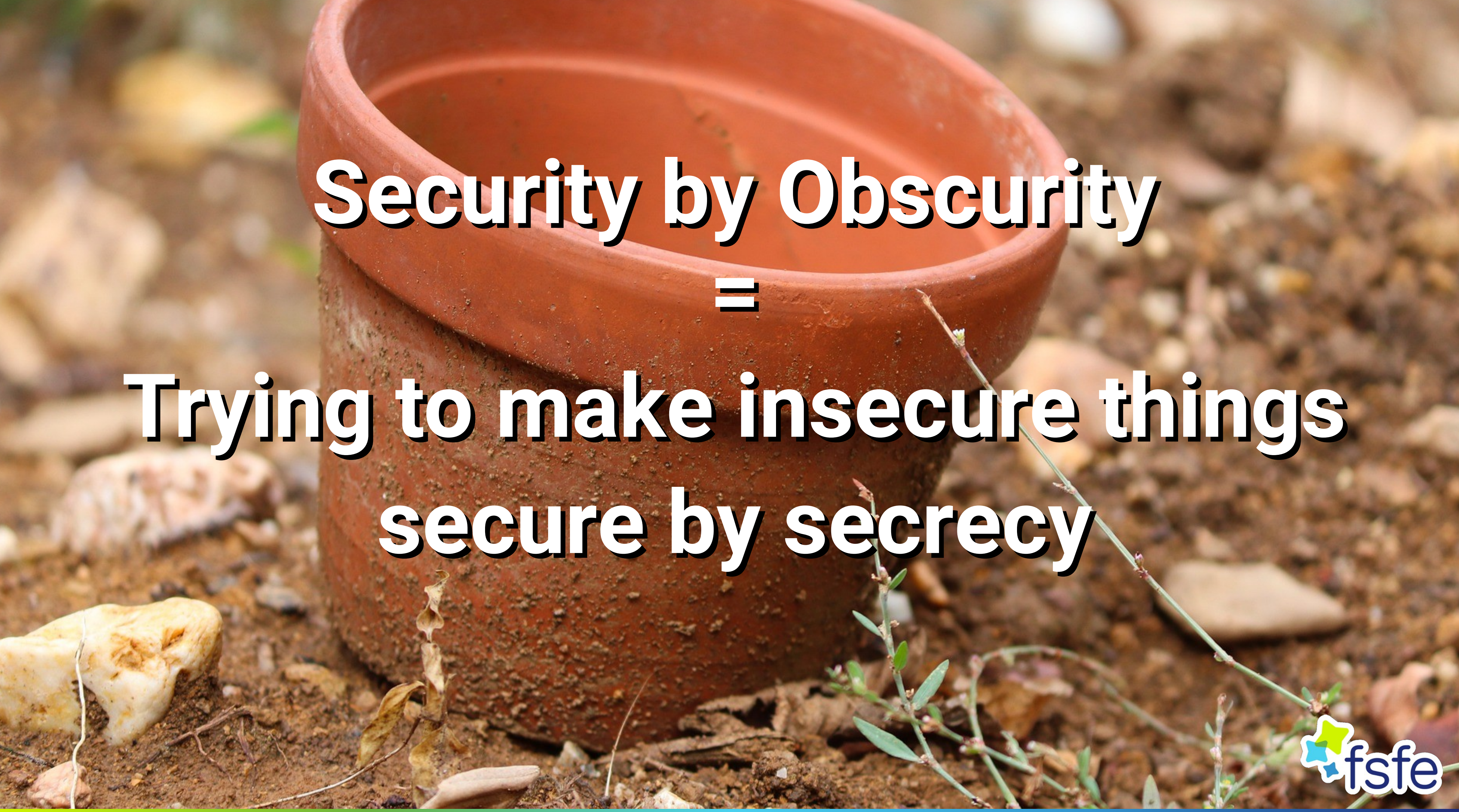
Improve

Software can be modified by everyone, for the better or the worse

fsfe

„There might be areas that we see as too critical for whatever reason to publish, usually related to cyber security.“

– Thomas Gageik, European Commission



Security by Obscurity

=

Trying to make insecure things secure by secrecy

Flaws of Security by Obscurity

- Secrecy itself is no sufficient protection
  - Human factor (stupidity, betrayers)
  - Brute-force
- Many examples in IT
  - Windows
  - Citrix
  - Meltdown, Spectre...

Kerckhoffs's Principle

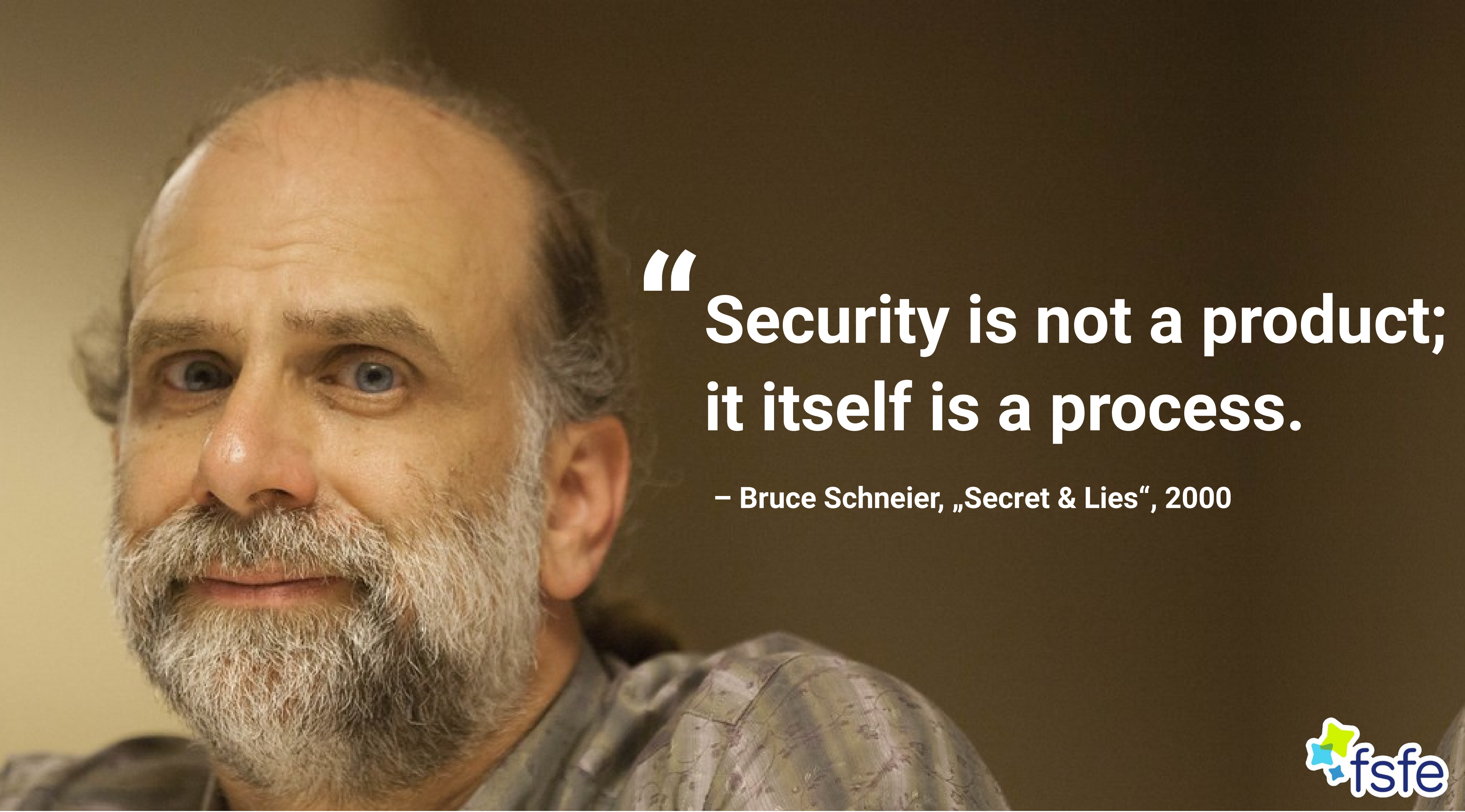
"[A cipher] should not require secrecy, and it should not be a problem if it falls into enemy hands"

– Auguste Kerckhoffs, 1883

Shobha
&
NAV-TAL

STOP
ALL WAY

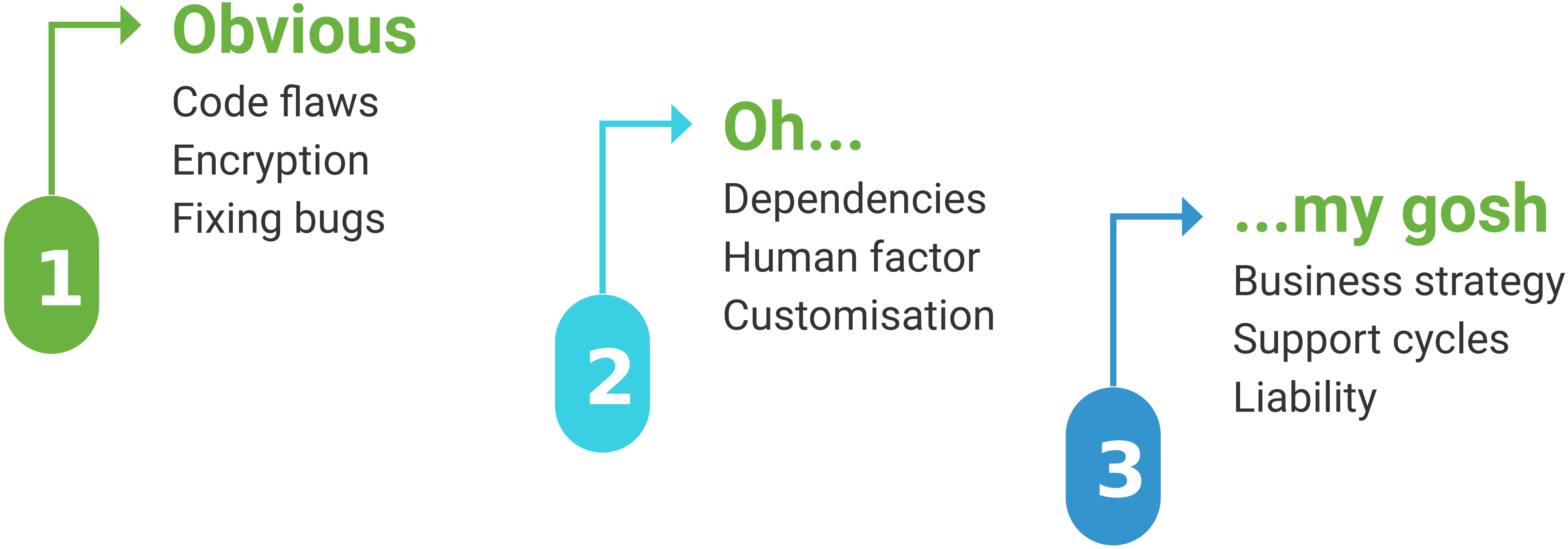
CYBER CYBER SECURITY



“Security is not a product; it itself is a process.

– Bruce Schneier, „Secret & Lies“, 2000

IT Security as a Process



1

Obvious

Code flaws

Encryption

Fixing bugs

2

Oh...

Dependencies

Human factor

Customisation

3

...my gosh

Business strategy

Support cycles

Liability

Free Software as a Solution?

AGPLv3
Free Software
LGPLv3
Free Software
GPLv3
Free Software
?

Security Benefits by Free Software

Transparency

Independent security audits increase trust, externally and internally

Code Quality

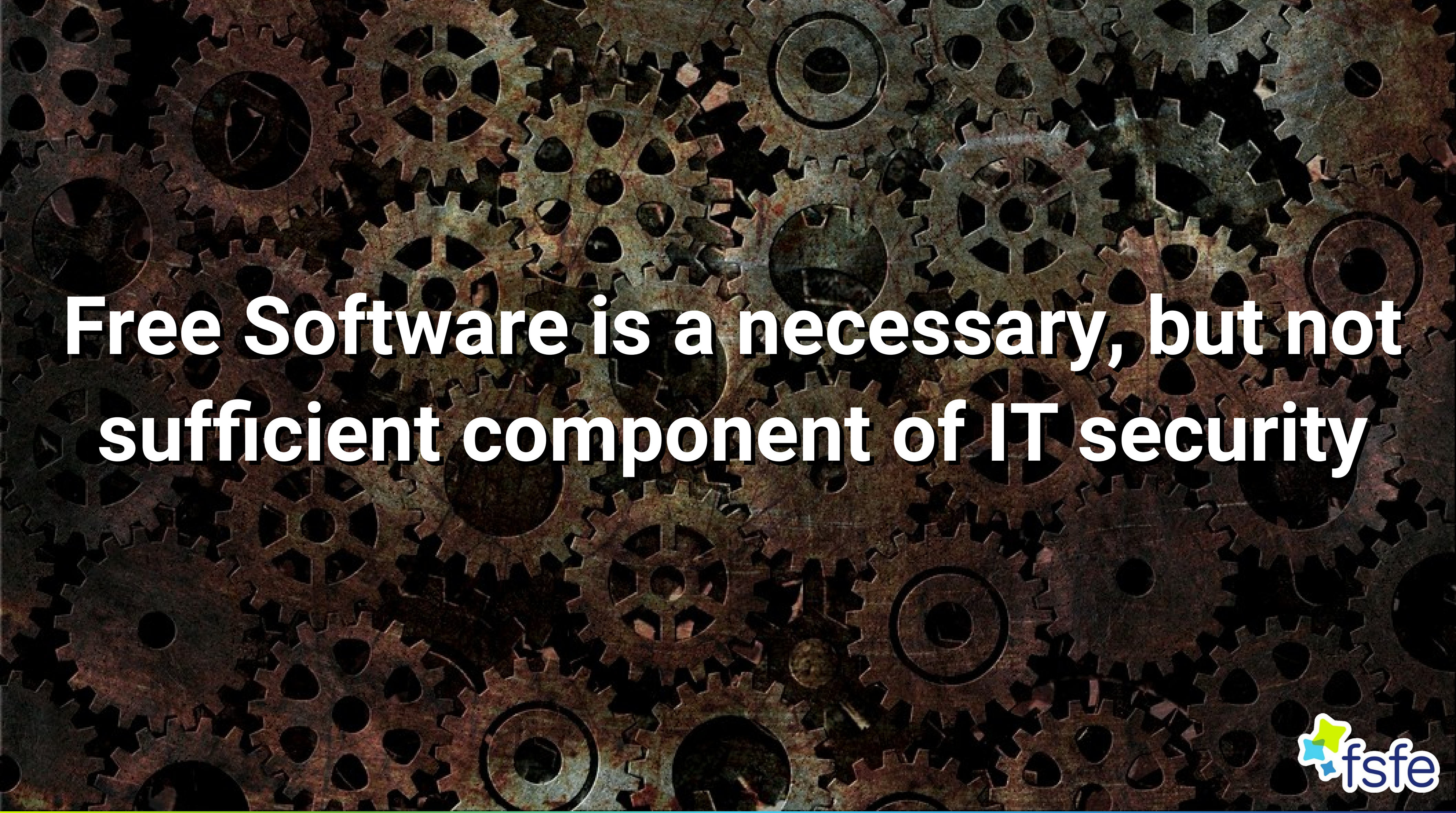
Better take a closer look before publishing code, and follow best practices

Synergy

Other users and the community take interest and can contribute

Independence

Issues can be solved on one‘s own. Forking possible if necessary



Free Software is a necessary, but not sufficient component of IT security

Challenges

Responsibilities

Who takes care of security, especially in shared projects?

Dependencies

How many external components can be handled?

Threats

Can you make yourself vulnerable by „too much“ openness?

Resources

Critical components are often underfinanced. How to handle that?

Our Demands

- Free Software for **critical infrastructure**
  - Trust, transparency, accountability
- **Public Money → Public Code**
  - High priority for digital sovereignty
- More **sense of responsibility** by companies and states regarding Free Software components

Thank you! Questions?

Thanks to all supporters of the FSFE who enable our work.

Become a part of it!

fsfe.org/support

Legal information

- Slides licensed under CC-BY-SA-4.0 unless stated otherwise
- FontAwesome icons v4.7.0 by Dave Gandy under SIL OFL 1.1
- Picture of Bruce Schneier by Terry Robinson, CC-BY-SA-2.0