



Digital Sovereignty

BE-CYBER

22 September 2026

Bart Preneel, COSIC, KU Leuven



EU Digital Sovereignty (circa 2020)

- Strategic autonomy — the capacity to make sovereign choices about technology without being subject to foreign jurisdictional overreach or supply chain dependency
- June 2026: Communication on European Tech Sovereignty, accompanied by an EU Open Source Strategy
- Economic:
 - data (GDPR)
 - infrastructure (e.g. 5G, NIS2, Chips Act, CRA)
 - markets (DMA)
- Normative (self-determination): fundamental rights, democracy, rule of law
 - GDPR, AI Act

EU Digital Sovereignty challenges

- Dominant position of Big Tech: cloud, social media, AI
 - enforcement is hard: GDPR, AI Act
- Hybrid warfare in digital domain: intelligence (cars, cameras), hacking
- Geopolitics: stop access at any time (e.g. Mythos and Fable, solar invertors,...)

EU Digital Sovereignty in numbers

- 40% of Microsoft's revenue comes from Europe
- AI investment:
 - Big tech: \$700 B in 2026 and \$ 1000 B in 2027
 - EU plans €30 B for AI gigafactories in 2027 (2/3 from private sector)
- Chips act (2023): increase EU's share of global semiconductor production from 10% to 20% (€ 43B target not reached)
 - Chips act 2.0 reoriented towards cloud and AI Development Act (CADA)
- EU Open Source strategy: no budget yet

How to achieve a trustworthy supply chain for software and hardware?

Hard National Security Choices

LAWFARE

☰ TOPICS

HOME

FOB BLOG

JAN. 6 PROJECT

REVIEWS AND ESSAYS ▼

AEGIS

RESOURCE PAGES ▼

MORE ▼

TRUSTWORTHINESS IN HARDWARE AND SOFTWARE

How Can One Know When To Trust Hardware and Software?

By **Paul Rosenzweig, Benjamin Wittes** Monday, May 2, 2022, 3:36 PM

<https://s3.documentcloud.org/documents/21831749/creating-a-framework-for-supply-chain-trust-in-hardware-and-software.pdf>

Axiomatic Basis of Trust

Accept without evidence

- Reputation of source
- ISO certified
- People certified

Based on accountability

- Institutions
- Processes

Supply chain source selection

- Secret purchase
- Random selection

Analytic Basis of Trust

Observation

- Testing

Deductive

- Verification
- Model checking

Synthesized Basis of Trust:

based on components and the way they are put together

Smaller trusted
computing base

- e.g. hypervisor

Split device
fabrication

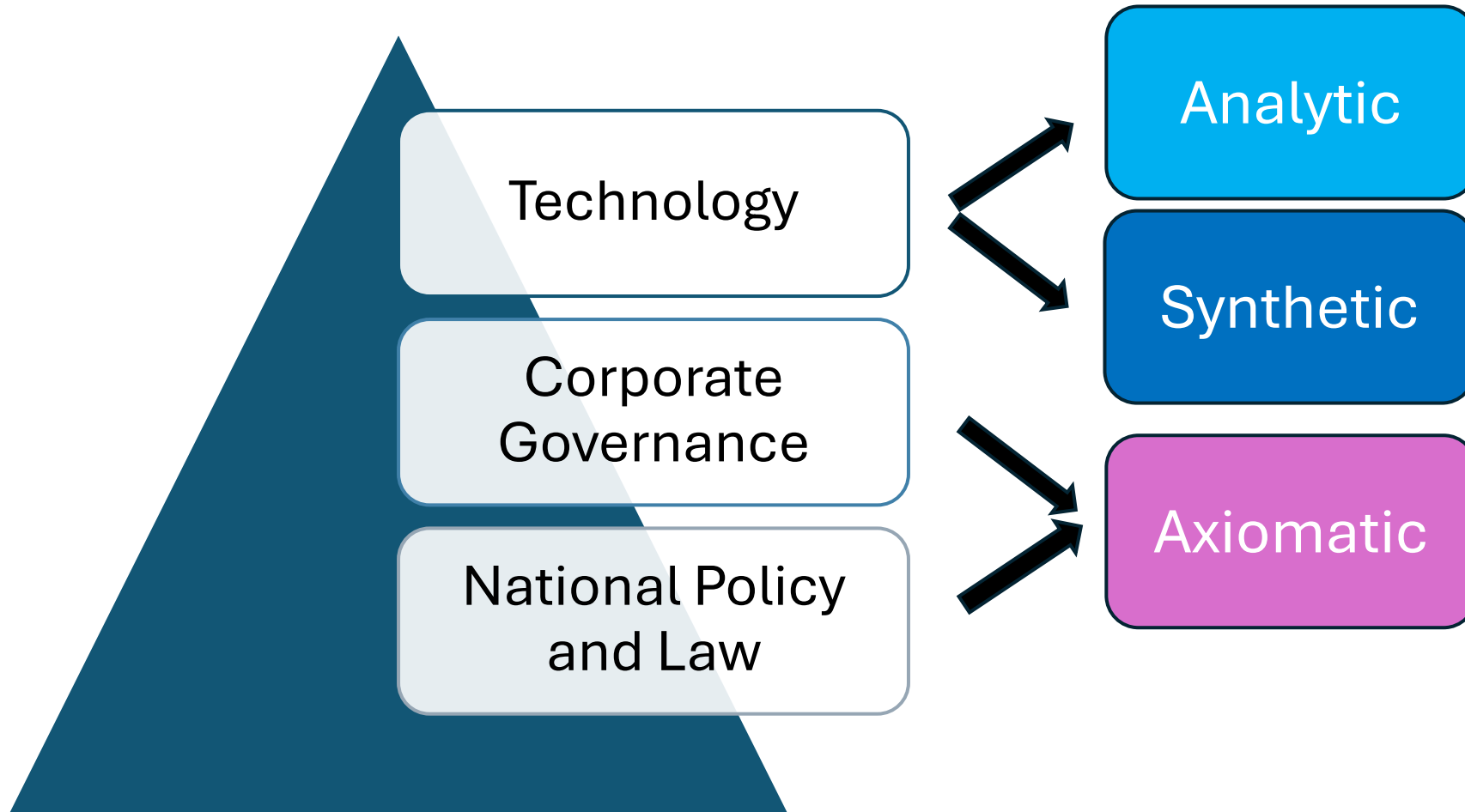
Fault tolerant
systems

- blockchains
- secure MPC

Secure composition

External monitor for catastrophic failures

Mapping



Towards a Framework to Evaluate Trust

Transparency

Accountability

Independent
evaluation

Provable analytic
verification rather
than axiomatic non-
verifiable approach

Bart Preneel

ADDRESS: Kasteelpark Arenberg 10, 3000 Leuven

WEBSITE: homes.esat.kuleuven.be/~preneel/

EMAIL: Bart.Preneel@esat.kuleuven.be

MASTODON: [bpreneel@infosec.exchange](https://infosec.exchange/@bpreneel1)

TWITTER: [@bpreneel1](https://twitter.com/bpreneel1)

TELEPHONE: +32 16 321148

KU LEUVEN

ArenBerg Crypto
BV

COSIC

