Sovereignty

Digital Humanism?

23 Sept 2022

Paul Timmers

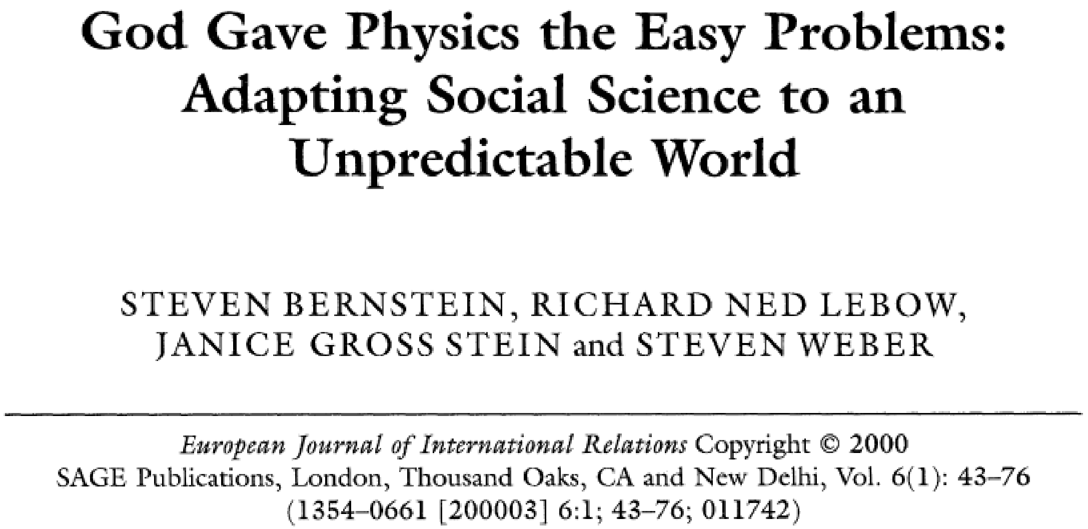
Research Associate Oxford University/Oxford Internet Institute,

Adjunct Professor European University Cyprus

Former Director European Commission Digital Society, Trust and Cybersecurity

[*paul.timmers@iivii.eu*](mailto:paul.timmers@iivii.eu)

Credits old rubber font: https://www.dafont.com/



God Gave Physics the Easy Problems: Adapting Social Science to an Unpredictable World

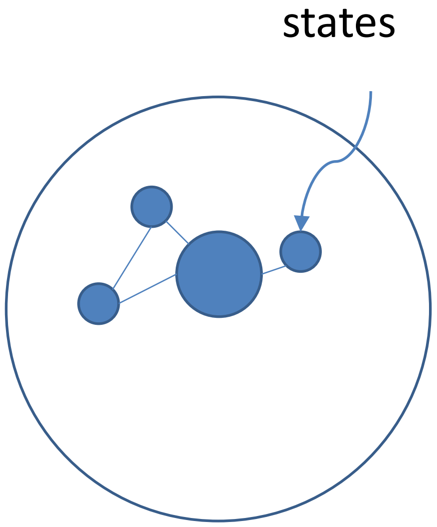
STEVEN BERNSTEIN, RICHARD NED LEBOW,
JANICE GROSS STEIN and STEVEN WEBER

European Journal of International Relations Copyright © 2000
SAGE Publications, London, Thousand Oaks, CA and New Delhi, Vol. 6(1): 43–76
(1354–0661 [200003] 6:1; 43–76; 011742)

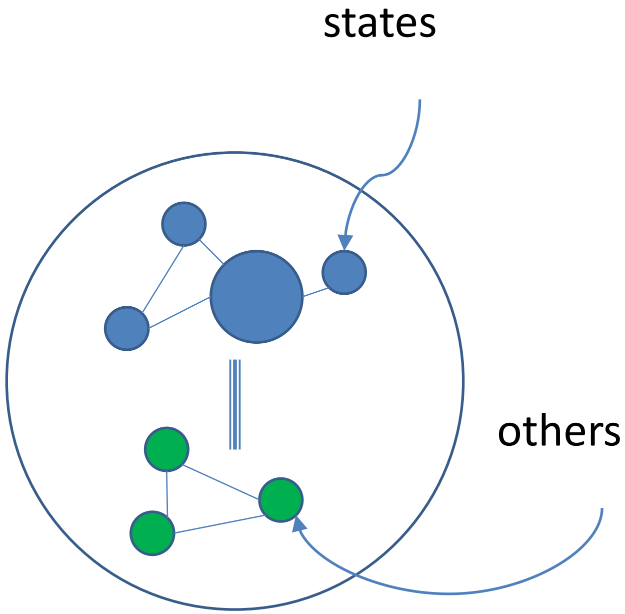
International relations theories

- **Realist**
  - Anarchy of states, security dilemma, state of war is ‘natural’, hegemons
- **Liberalist**
  - More than states, cooperation is possible
- **Constructivist**
  - It depends on human nature, identity, socialization
- Others
  - identity, territory

Three schools

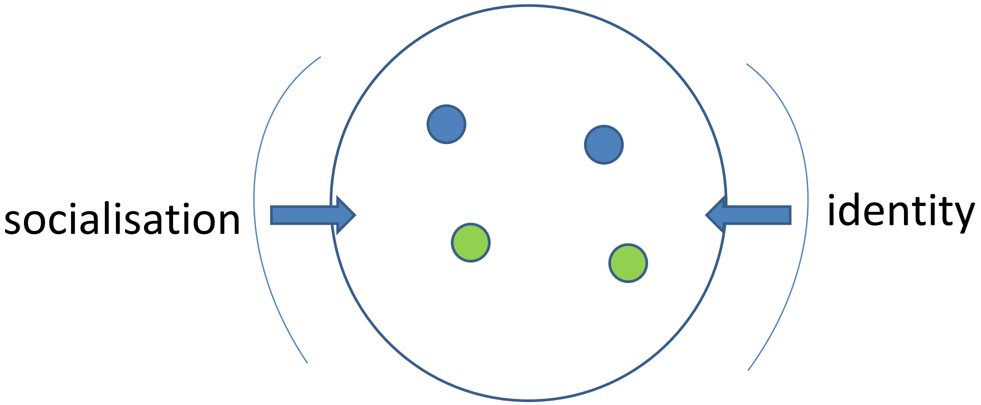


Realism



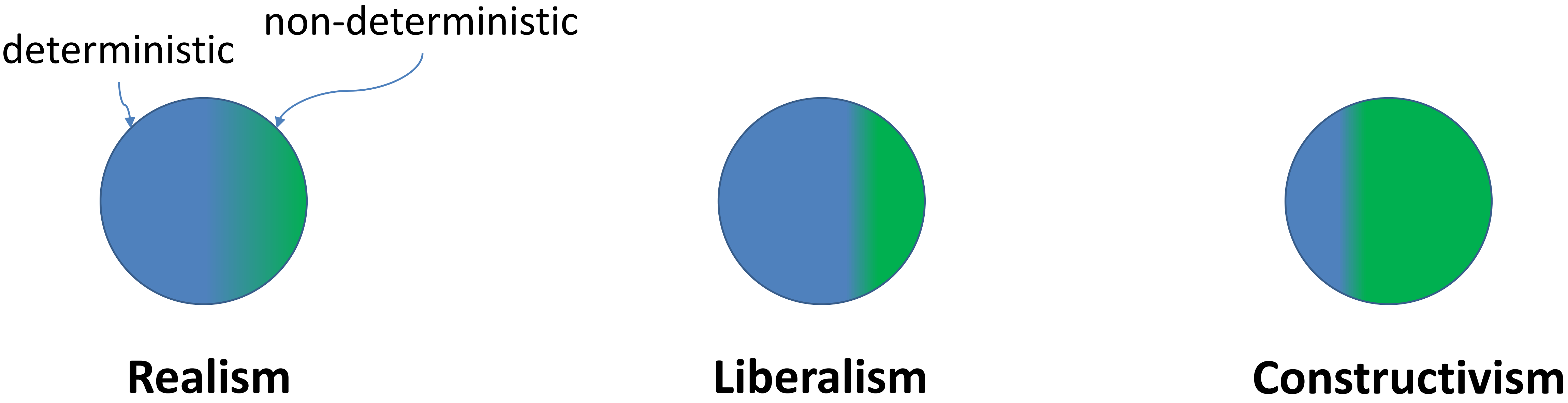
Liberalism

Digital Humanism?



Constructivism

Deterministic or Non-deterministic



deterministic

non-deterministic

Realism

Liberalism

Constructivism

Digital Humanism?

Some more IR background

- ‘Why war?’
- International relations, game theory, governance
- Technology and international relations:
  - Technology as exogeneous factor
  - Technology as source of power
  - Techno-Politics as two-way interplay (an emerging theory)

Sovereignty

- 1648 Peace of Westphalia, Bodin, Hobbes, Rousseau…

- Shared and pooled sovereignty as in EU

Picture: Armistice. (2022, August 19). In *Wikipedia*. https://en.wikipedia.org/wiki/Armistice

State Sovereignty

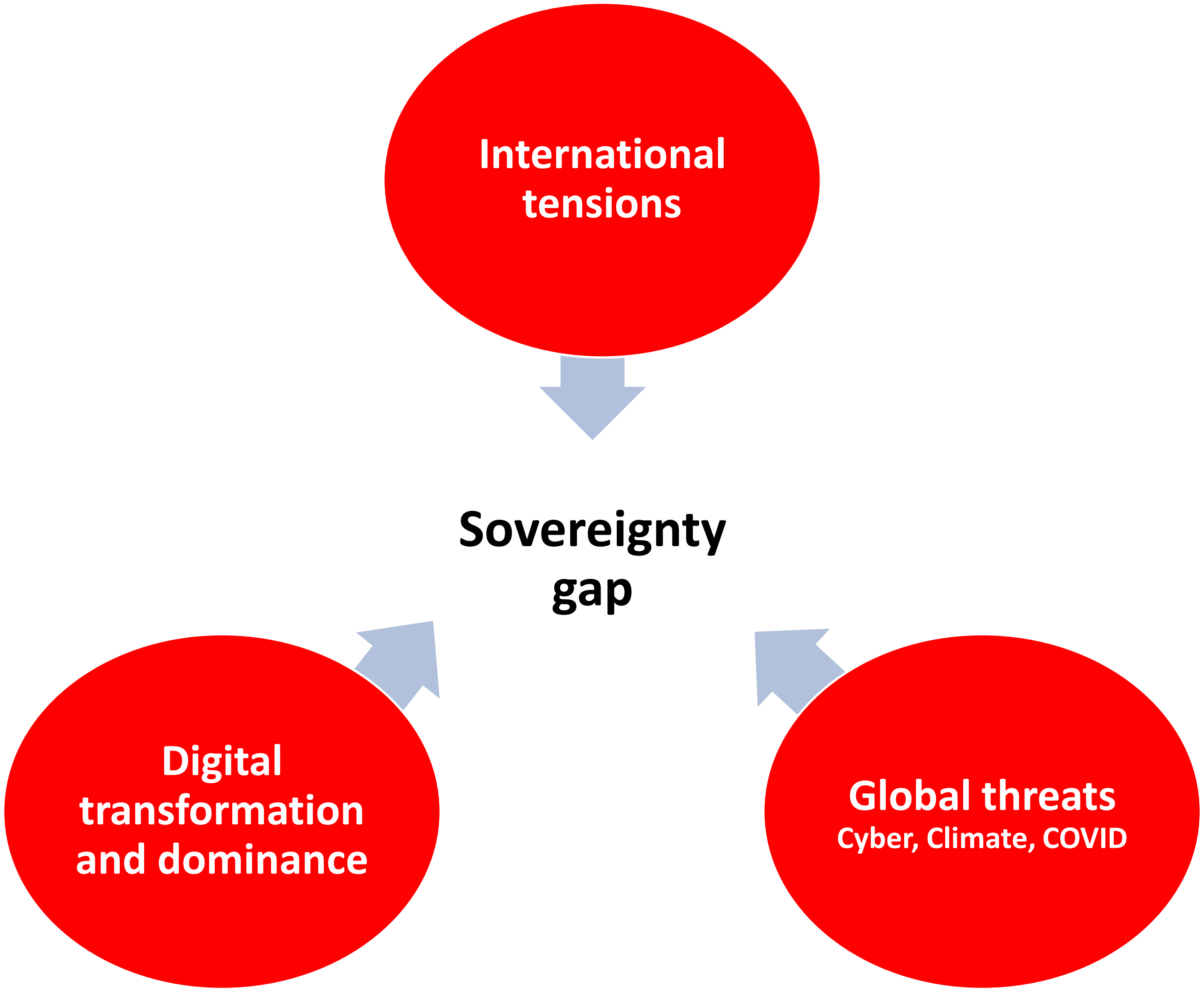
State sovereignty is foundational, institutional, and territorial:

- authority, recognition
- internal legitimacy between state and citizens
- external legitimacy of the state versus foreign states
- territory, natural and digital resources “that belong to us”
- people, values, culture.

Sovereignty of the individual may link to state sovereignty

Sources: Adler-Nissen (2008), Biersteker (2012), Bickerton (2022)

Why is sovereignty a concern?



International tensions

Sovereignty gap

Digital transformation and dominance

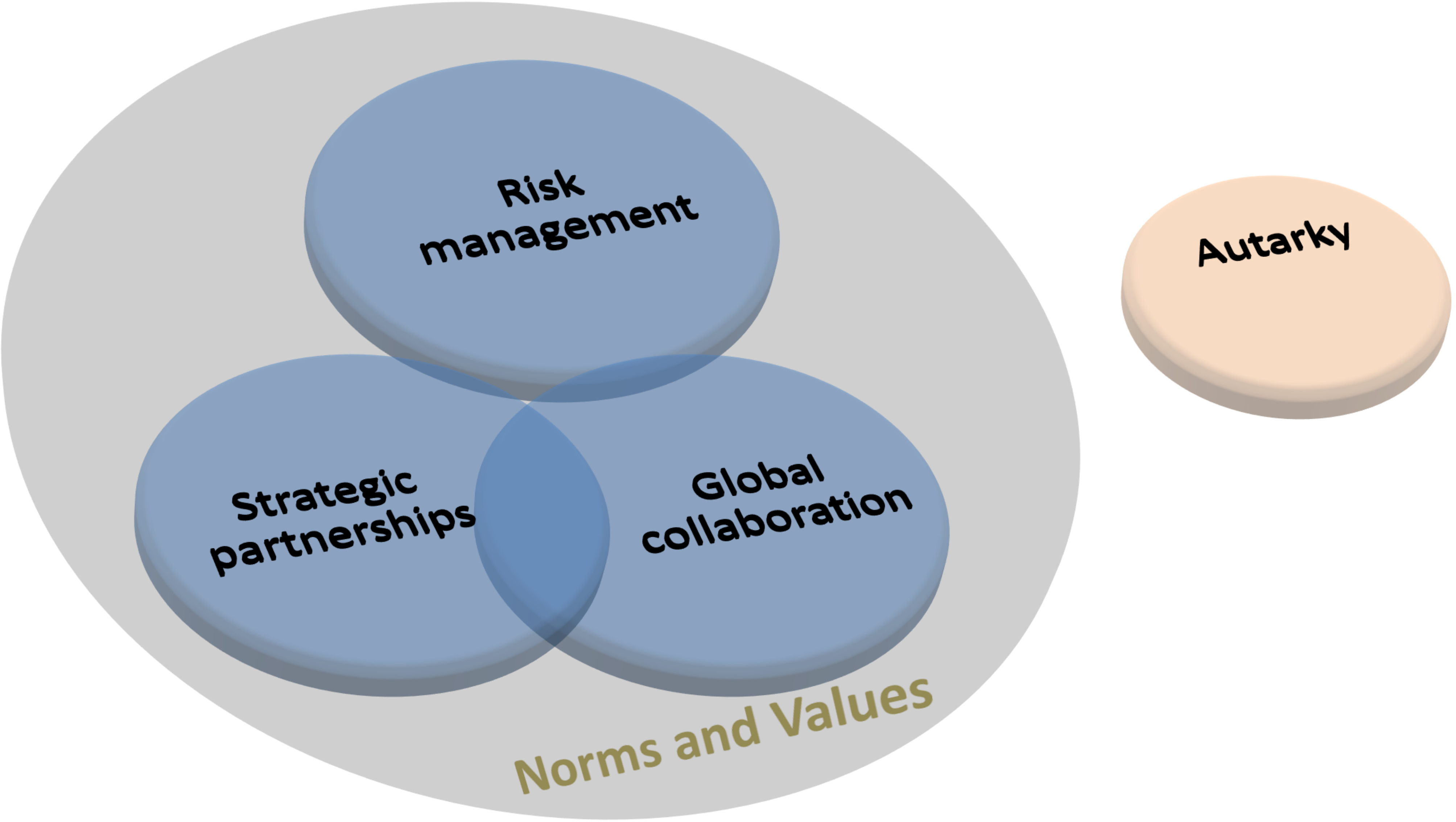
Global threats
Cyber, Climate, COVID

Source: Timmers (2019); Kello (2017)

Strategic autonomy

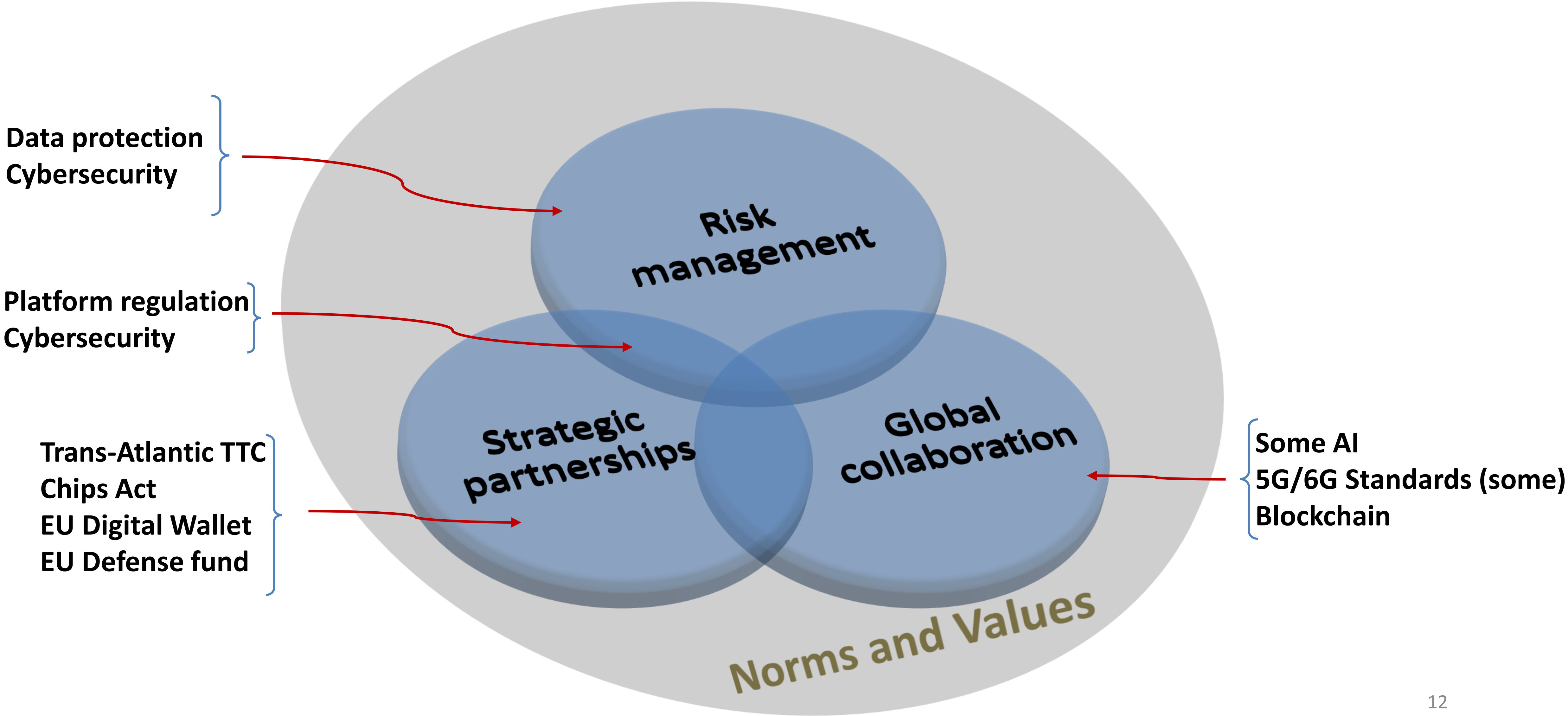
- Strategic autonomy is the means to the end, namely sovereignty
- Consists of **Control**, **Capabilities** and **Capacities** (C3) to decide and act on essential aspects of our economy, society and democracy
- Is explicit or implicit driver of foreign, defence, industrial, digital policy
  - In the EU: EU Chips Act, EU digital wallet, Digital Markets Act, COVID Pass, European Critical Raw Materials Act,…

Strategies for Strategic Autonomy



Sources: Timmers (2019)

EU and strategic autonomy



Sources: Timmers (2019)

Strategic autonomy and international relations are in mutual interplay

- EU COVID Pass, adopted by over 60 countries, 1 billion people
- EU in international standards (5G, IoT, …) and UN cyber-diplomacy
- Brussels effect – GDPR (Bradford)

- But what about military power?
- What about a Beijing effect?
- …

Strategic autonomy fallacies

1. ‘Don’t think of autarky’

2. ‘We can have it all’

3. ‘Let’s take back control’

Picture sources: (1), (2) licensed under CC BY-SA; (3) https://greenagenda.org.au

Digital Dependency Index

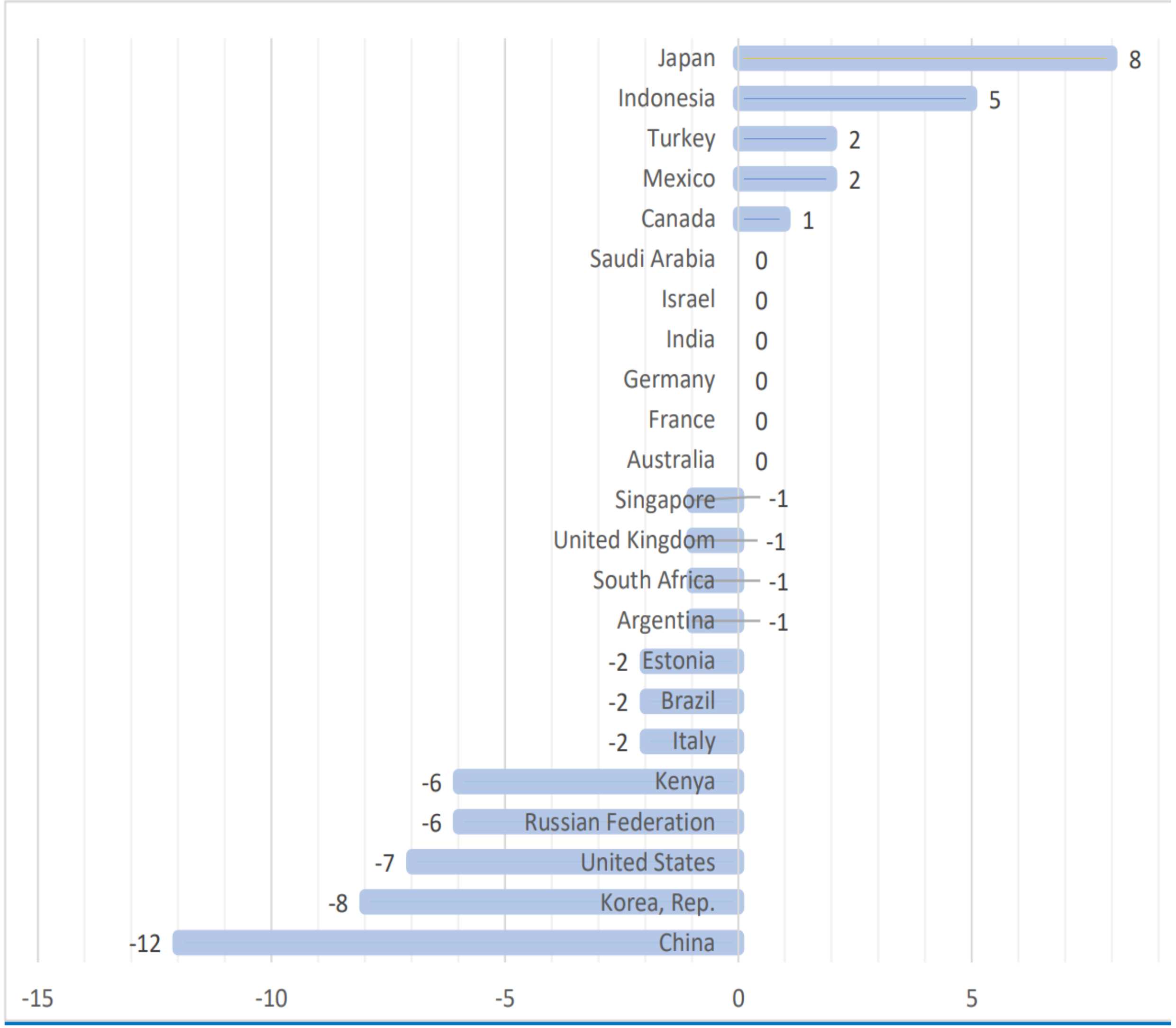


Figure 7. Change of DDI Value (Equally Weighted) between 2010 and 2019 (in percentage points)

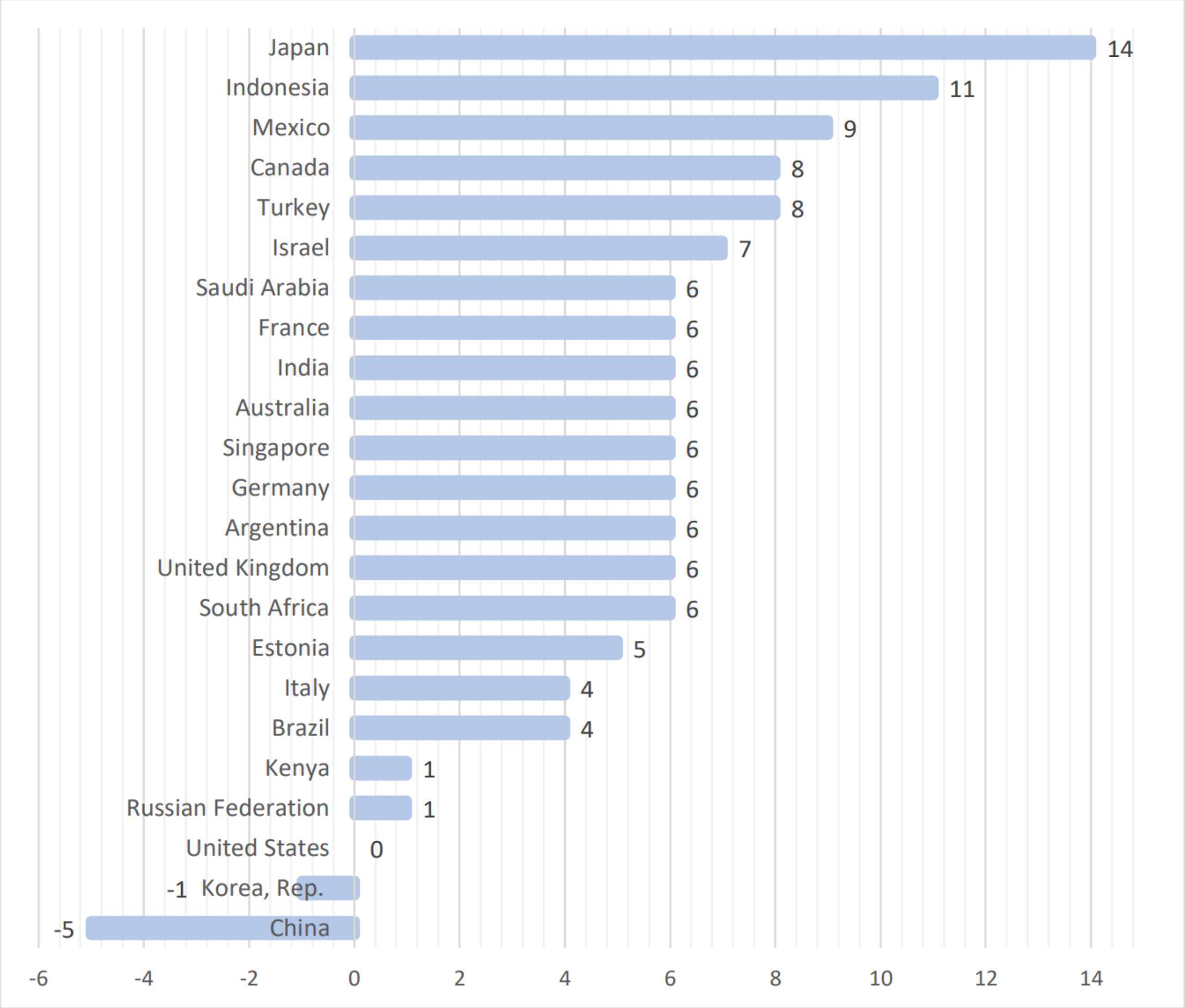
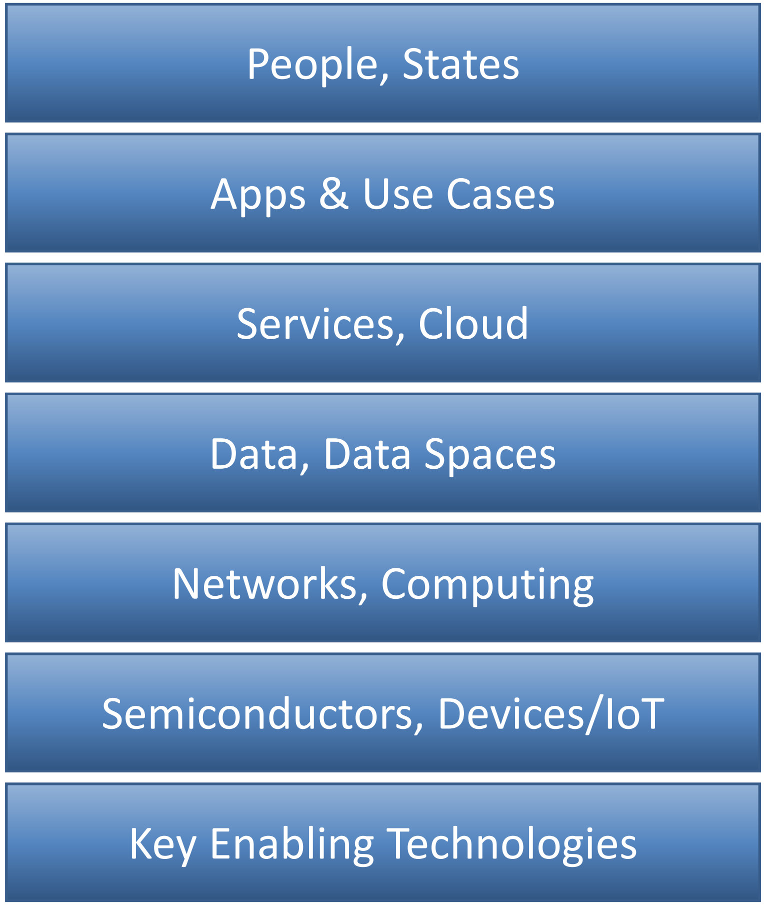


Figure 8. Change of autonomy gap vis-à-vis USA between 2010 and 2019 (in percentage points)

Sources: Maximilian & Yen-Chi, Konrad Audenauer Stiftung (2022)

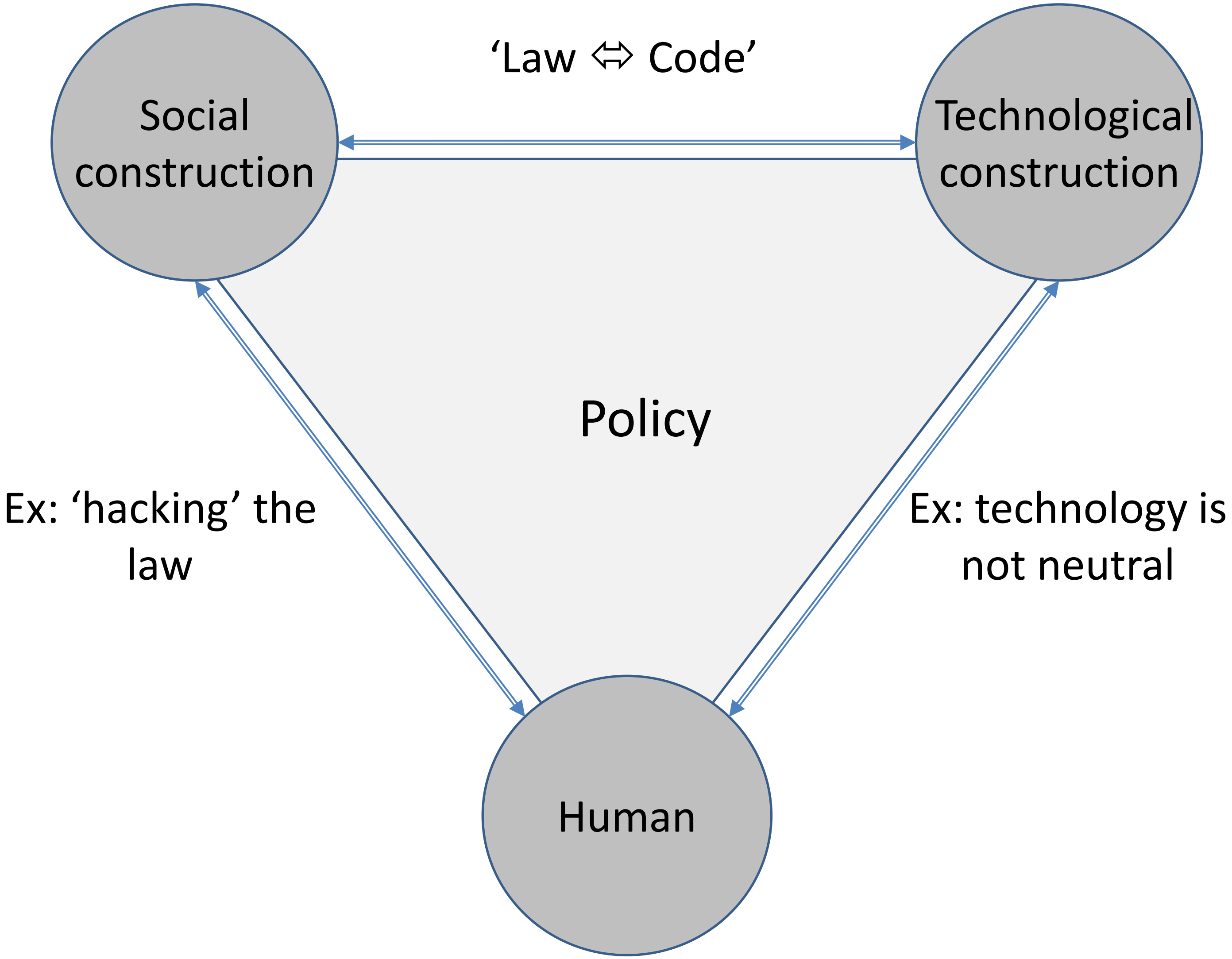
Digital Strategic Autonomy (digital sovereignty) has a dilemma of choice



People, States	
Apps & Use Cases	Integration (drones, Industry 4.0, smart cars…), applied AI, metaverse
Services, Cloud	Trusted cloud, sovereign eID, blockchain, confidential computing, AI, digital twins
Data, Data Spaces	Platforms, supply chain security, basic cloud
Networks, Computing	5G/6G, supercomputing, AI, edge cloud & computing
Semiconductors, Devices/IoT	Semiconductors, IoT, secure hardware, embedded AI
Key Enabling Technologies	Quantum, secure open source, semiconductors

Sources: Timmers (2022)

Social and Technological Construction



‘Law ⇔ Code’

Social construction

Technological construction

Policy

Ex: ‘hacking’ the law

Ex: technology is not neutral

Human

Hannes Werthner
Erich Prem
Edward A. Lee
Carlo Ghezzi *Editors*

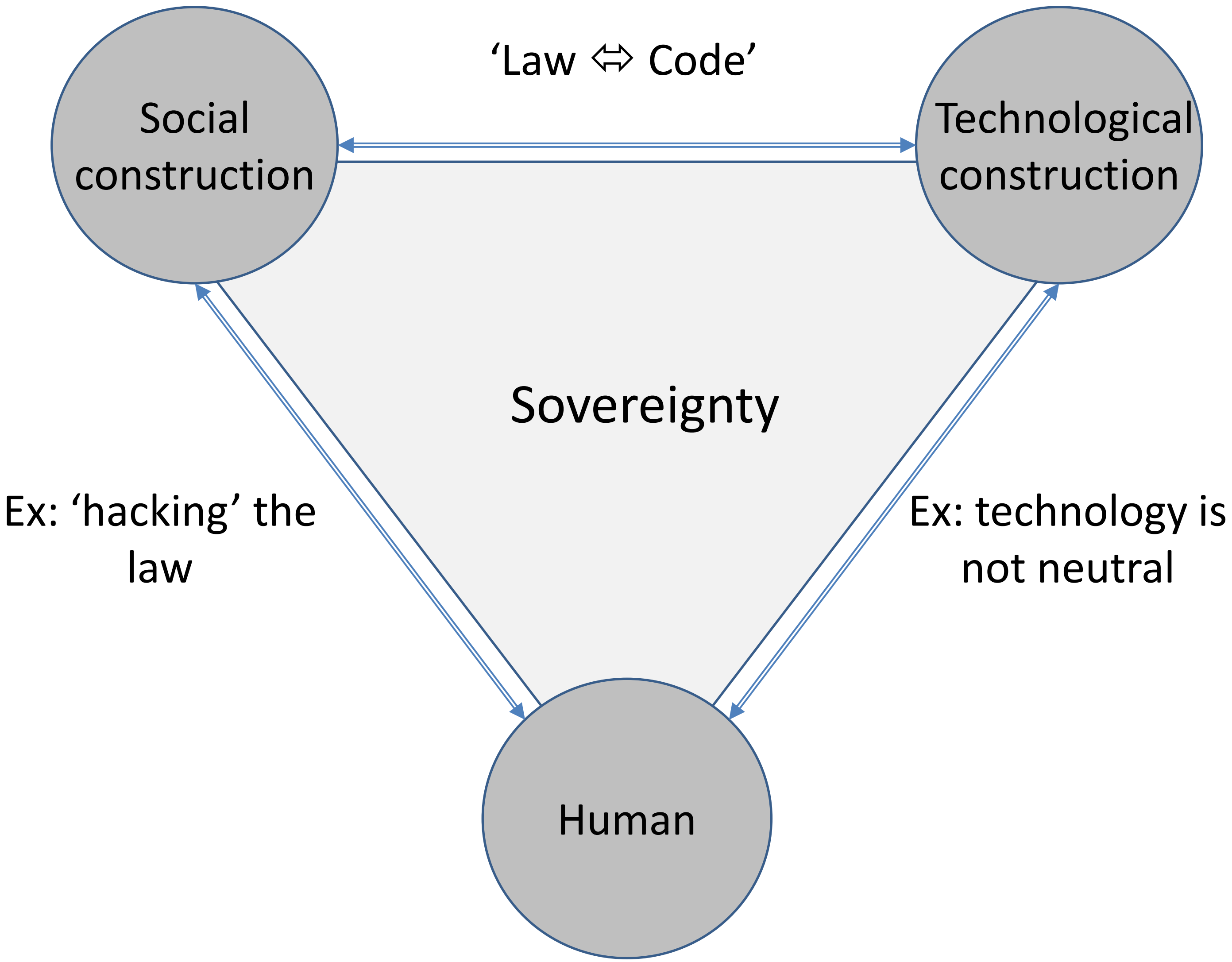
Perspectives on Digital Humanism

OPEN ACCESS

Springer

Sources: Berger & Luckmann (1966), Lessig (200), Cohen (2017), De Filipi (2019), Timmers in Perspectives on Digital Humanism (2022)

Social and Technological Construction



‘Law ⇔ Code’

Social construction

Technological construction

Sovereignty

Ex: ‘hacking’ the law

Ex: technology is not neutral

Human

Hannes Werthner
Erich Prem
Edward A. Lee
Carlo Ghezzi *Editors*

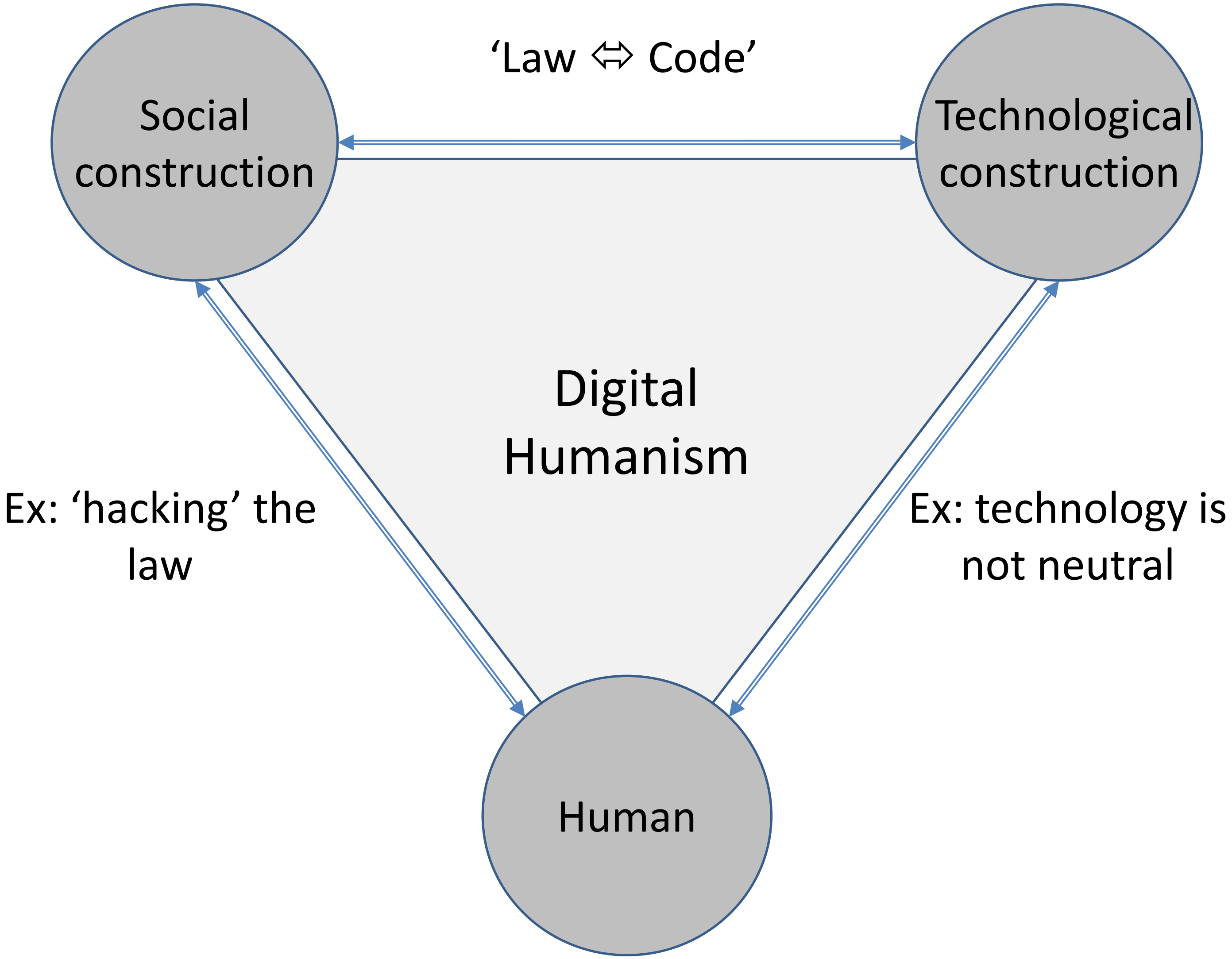
Perspectives on Digital Humanism

OPEN ACCESS

Springer

Sources: Berger & Luckmann (1966), Lessig (200), Cohen (2017), De Filipi (2019), Timmers in Perspectives on Digital Humanism (2022)

Social and Technological Construction



‘Law ⇔ Code’

Social construction

Technological construction

Digital Humanism

Ex: ‘hacking’ the law

Ex: technology is not neutral

Human

Hannes Werthner
Erich Prem
Edward A. Lee
Carlo Ghezzi *Editors*

Perspectives on Digital Humanism

OPEN ACCESS

Springer

Sources: Berger & Luckmann (1966), Lessig (200), Cohen (2017), De Filipi (2019), Timmers in Perspectives on Digital Humanism (2022)

Sovereignty in the digital age

- **Territorial**
  - Includes digital territory such as data, IP, .eu, domestic digital networks…
- **Institutional**
  - Digital and democracy, e-governance, tech alliances of like-minded…
- **Foundational**
  - Redefines ‘us’, ‘others’, power of digital platforms, self-sovereignty…

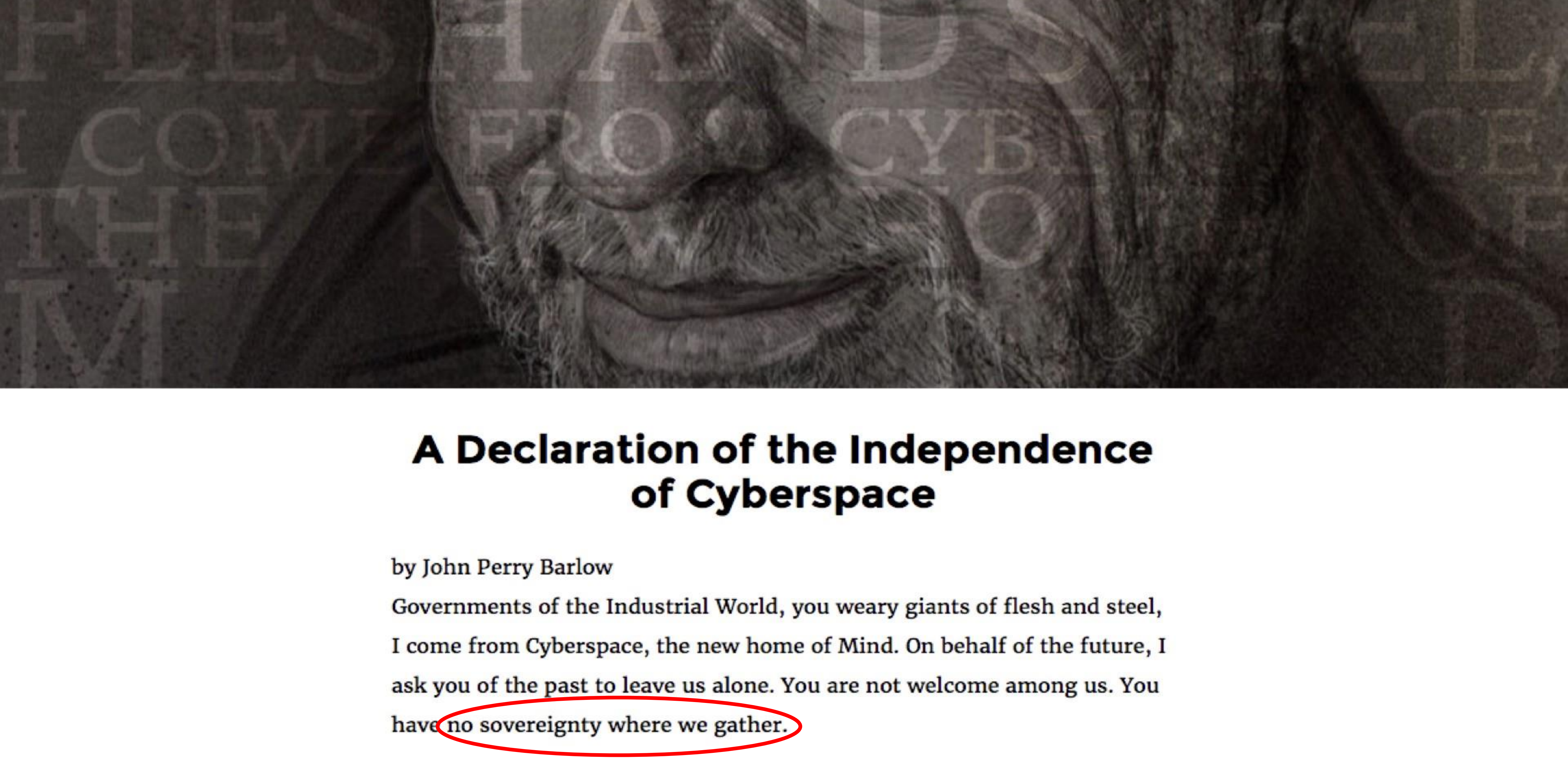
Digital and Sovereignty

Digital Humanism

- Digital is changing sovereignty conflicts
  - ‘unpeace’; cyber-kinetic warfare; commercial ICT@war

- Escaping the security dilemma and going beyond Westphalian sovereignty
  - New sovereignty: Internet (Barlow); network state (Afropolitan)
  - Global commons, e.g., Internet domain name management, .eu
  - Self-sovereignty, SOLID, IRMA, …
  - Beyond national security: EU NIS Directive, 5G security
  - Beyond national sovereignty: EU DSA, EU Media Freedom Act
  - Rethinking law as an instrument of sovereignty: NIS-AI and law

Sources: Kello, John Perry Barlow, Srinivisan, Forbes/Maria Gracia Santillana (2022-09-13



A Declaration of the Independence of Cyberspace

by John Perry Barlow

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

https://www.eff.org/cyberspace-independence

Digital sovereignty: Commission proposes Chips Act to confront semiconductor shortages and strengthen Europe's technological leadership

Brussels, 8 February 2022

Chips for Europe
R&D, pilots

Security of Supply
fabs

Monitoring and Crisis
Response

Sources: European Commission; This Photo by Unknown Author is licensed under CC BY-NC-ND

EU Chips Act

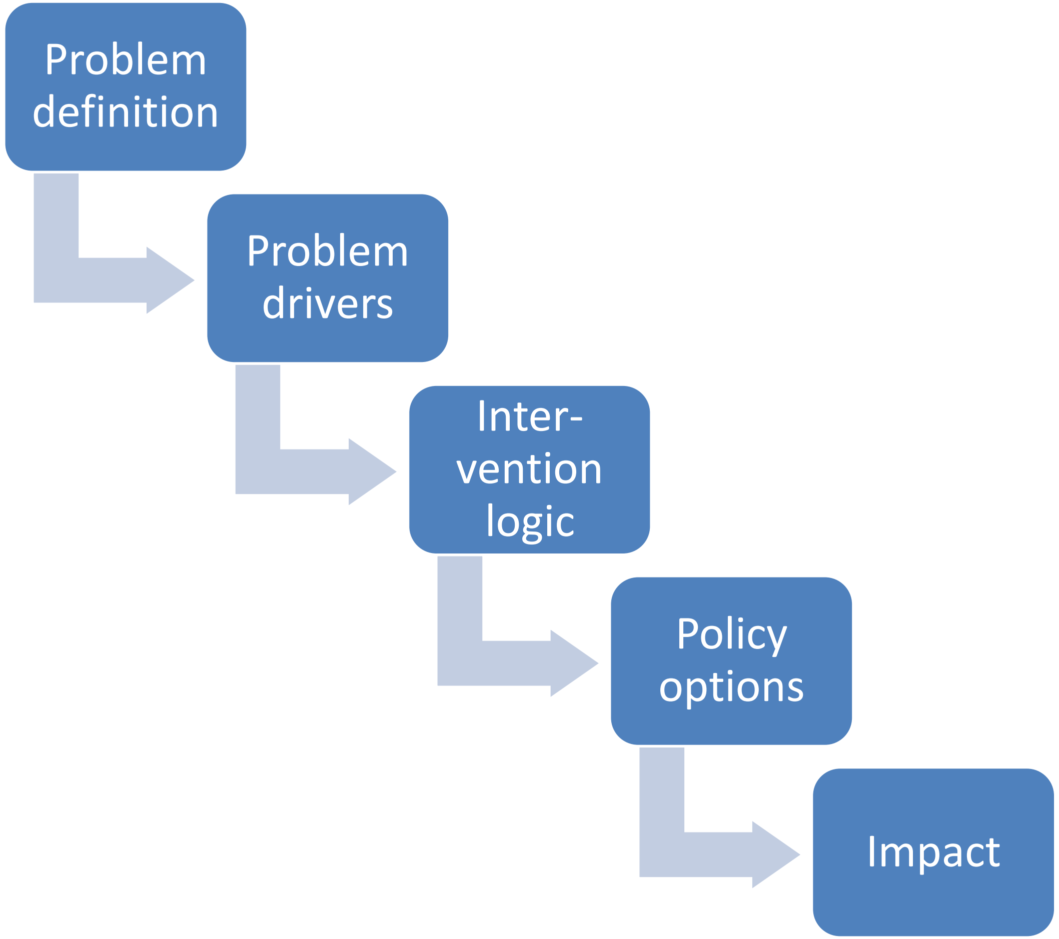
The most comprehensive approach to EU strategic autonomy so far

EU cannot go alone, it must at least be trans-Atlantic

Sovereignty conflicts

Sources: Timmers (2022) in Brookings Tech Stream

Let’s do an exercise in (EU) policy-making



- **ICT supply chain security**
- Driven by strategic autonomy, to safeguard sovereignty
  - **Capabilities**
  - **Capacities**
  - **Control**

ICT supply chain security

- **Problem**: vulnerable ICT supply chain
- **Drivers**: cyber-crime (Solarwinds attack), complex software supply chain (Log4j bug); Biden Executive Order, recent EU cybersecurity laws
- **Challenges**: build strategic autonomy, ensure resilience, sustain innovation
- **Specific challenges**: global business, China, USA, open source

- Policy toolbox: legislation, guidance, funding, cooperation, communication

The challenge of problem definition

do not attempt to read this 😉

- NIST: 'Federal departments and agencies become exposed to cybersecurity risks through the software and services that they acquire, deploy, use, and manage from their supply chain (which includes open source software components). Acquired software may contain known and unknown vulnerabilities as a result of the product architecture and development life cycle. Mitigating these types of risks throughout the supply chain is a cornerstone goal of the EO'

- NIS-2: Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures

- 5G toolbox: technical and, where relevant, non-technical factors. Technical factors may include cybersecurity vulnerabilities that may be exploited to gain unauthorised access to information (cyberespionage, be it for economic or political reasons) or for other malicious purposes (cyberattacks aimed at disrupting or destroying systems and data). Important aspects to consider should be the need to protect the networks across their entire lifecycle and the need to cover all relevant equipment, including in the design, development, procurement, deployment, operation and maintenance phases of 5G networks.
  Other factors may include regulatory or other requirements imposed on information and communications technologies equipment suppliers. An assessment of the significance of such factors would need to take into account, inter alia, the overall risk of influence by a third country, notably in relation to its model of governance, the absence of cooperation agreements on security, or similar arrangements, such as adequacy decisions, as regards data protection between the Union and the third country concerned, or whether this country is a party to multilateral, international or bilateral agreements on cybersecurity, the fight against cybercrime, or data protection.

Problem drivers

- Software development methods
- Commercial pressures
- Lack of security demand
- *Open source security practices*
- Global sourcing, also outside own jurisdiction
- Lack of control in updates and maintenance
- Lack of standards
- …

Show of hands – what is your preferred option?

1) no action

2) soft policy

3) hard law

4) hard law plus incentives

Suggestions for policy actions?

Policy toolbox: legislation, guidance, funding, cooperation, communication

EU Cyber Resilience Act has just been proposed, which has security labelling, standards, mandatory certification, monitoring, reporting, software updating; with some link to international cooperation, EU R&D and deployment funding

Takeaway
Should we have education on sovereignty in the digital age?

Pros

Cons

“My desire to be well-informed is currently at odds with my desire to remain sane.”

Time to discuss…

Credits: David Sipress, https://www.davidsipress.com/cartoons; McNamee, New Yorker, 2017