EU Digital Sovereignty: a Useful Concept or a Distraction?

A. Savin

CBS LAW

Why talk about this topic?

- The wrong answer: the ”buzz” generated
- The simple answer: loss of control over own security, data, platforms
- Difficulties not semantic, will not disappaer if we just find a better definition

What would I like to do here?

- Is there policy change? Change in laws?
- What do we do to regain control?

Where is the loss manifesting itself?

- Data: little to no control over data crossing borders, AI manipulation or purposes for which it is used
- Cybersecurity: more frequent, more deadly attacks
- Platforms: little possibility to rein in illegal (or legal but harmful) content

Key points

- Policy: EU does not incorporate sovereignty into its policy documents on digital regulation
- Discourse: EU talks a lot about sovereignty
- Laws: EU nevertheless takes steps to assert sovereignty according to common definitions, new laws *are* also about control

Definition?

- **legitimate control over the digital standards, data, software, infrastructure and services**

- **A set of tools for asserting regulatory power and maintaining strategic autonomy**

Definition?

- regulatory power
  - The power to reach those who need to be regulated – **extended scope of EU laws to non-EU actors**
  - The power to enforce laws: relevance of **EU agencies** (e.g. the Commission)

- strategic autonomy
  - The ability not to depend

Three manifestations of EU digital sovereignty

- The “Brussels effect”: control over territorial scope of its laws & the ability to impose their application
- Universal acceptance (because the solutions are good ?)
- The ability to regulate increasingly large number of platforms

Three examples where it is lacking

- Cyberattacks
- Content is created in the US, largest digital businesses all non-EU
- Platforms have the financial capacity to innovate around EU laws

EU Regulatory Framework & Digital Sovereignty

- Not defined in the old pillars (ECD, EECC, AVMSD)
- Not in 2015 DSM
- 2020 DSM
  - Integrity and resilience
  - Ability to develop own capacity
  - Ability to define own rules
- The 2021 Digital Compass: incoherent and clichéd

What is ***new*** in EU laws today

- *Ex ante* approach (DMA, AI Act)
- Asymetric regulation (DSA)
- Risk-based compliance (DSA, DMA, NIS2…)
- Massive increase in sector-specific regulation = less certainty about interplay between laws

1 Control over data

- Low investment and adoption of AI compared to China
- Low talent attraction, less patent applications than US

  = dependence on foreign technology

- Massive amounts of data in the control of Google, Apple, Facebook, Amazon and Microsoft

  = dependence on foreign platforms

1 Control over data

- Actions that need to be taken:
  - GDPR review
  - More sector-specific rules
  - ePrivacy Directive review

2 Cybersecurity

- Reliance on Chinese infrastructure
- Reliance on cloud solutions based abroad
- Actions
  - Gaia-X: an EU initiative for cloud sovereignty
  - NIS2
  - Cybersecurity Act
  - Common EU approach to 5G security

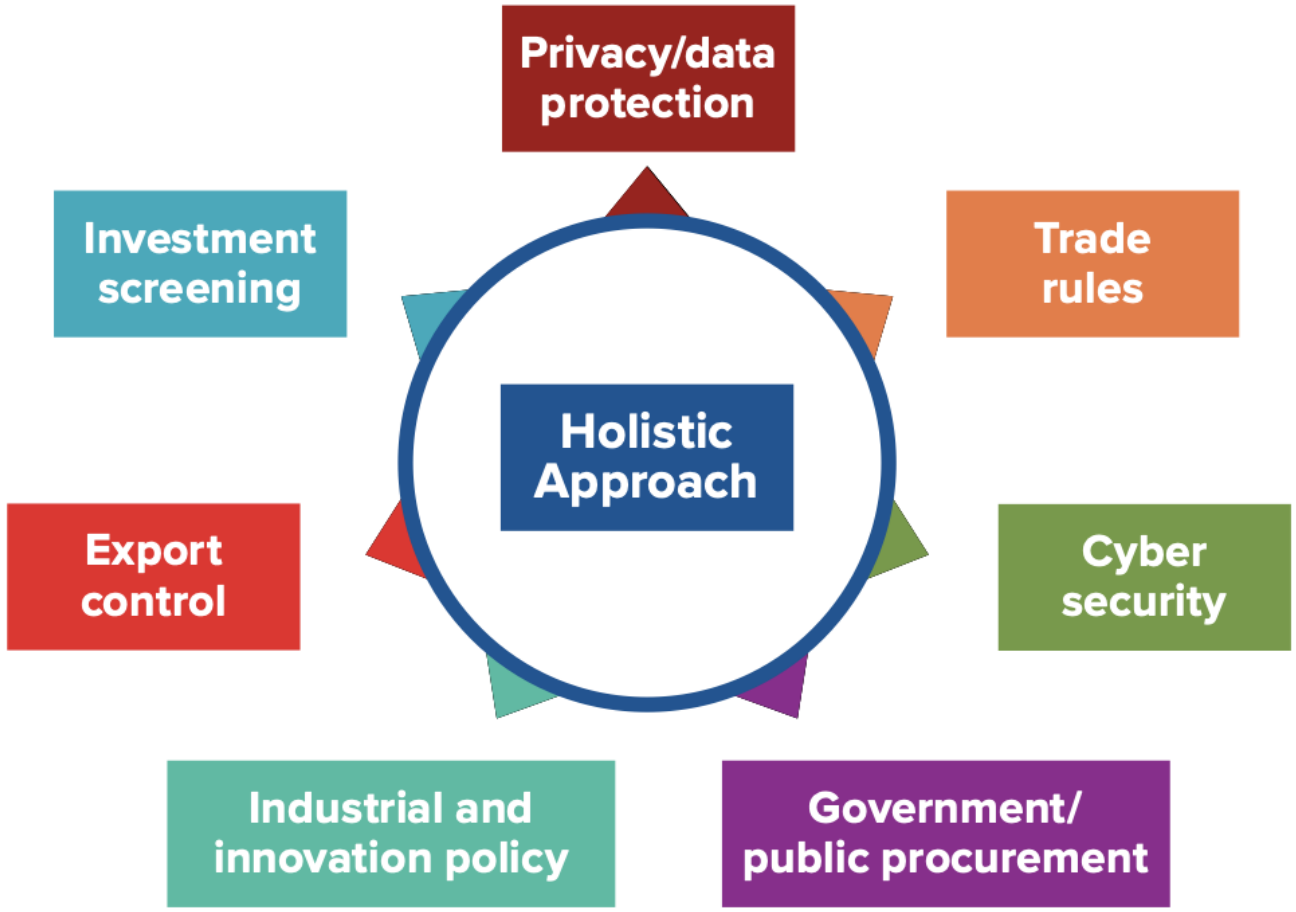
2 Cybersecurity

- Actions to be taken or need to be taken
  - Procurement
  - Better Certification
  - Better Coordination

3 Control over platforms

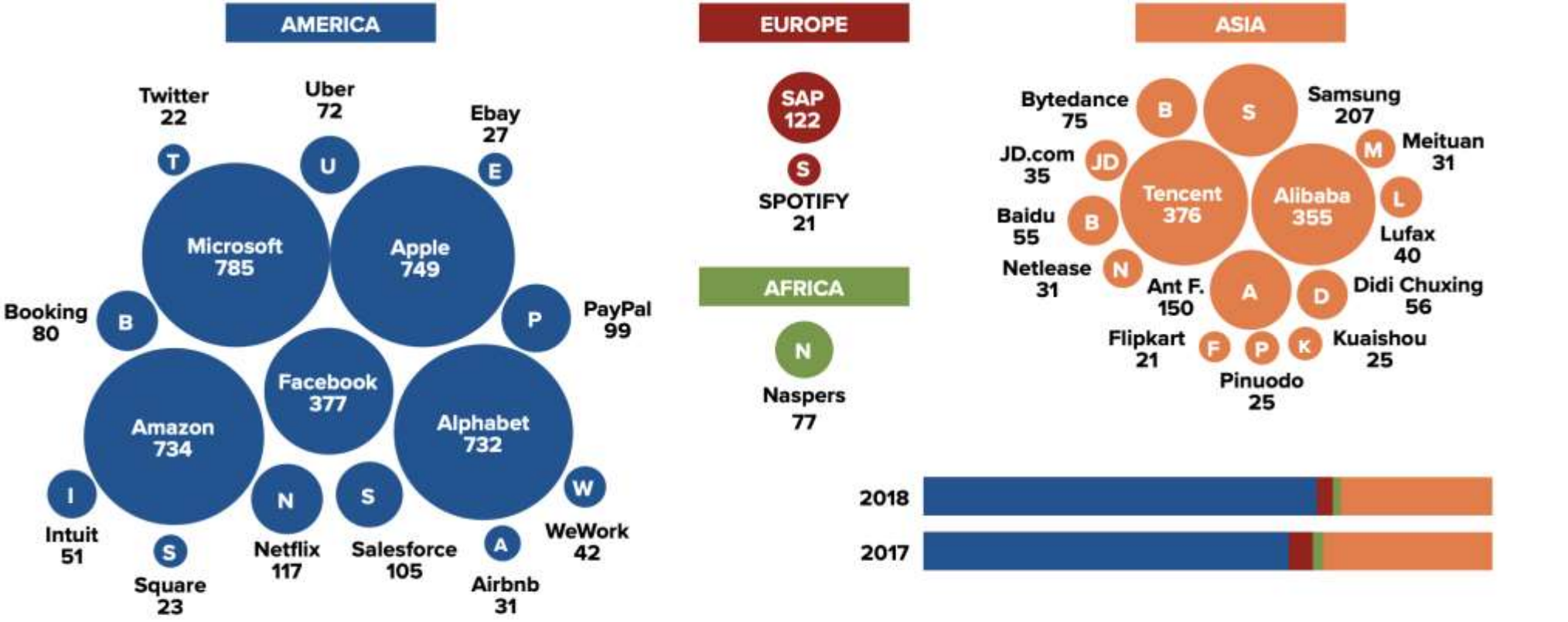
- DSA
  - Risk-based regulation of VLOPs
  - Meaningful sanctions
  - But, uncertain national **enforcement**
- DMA
  - Ex ante control of gatekeepers
  - But, **no enforcement expirience**

EU outline of policy tools for protecting digital sovereignty



Atlantic Council

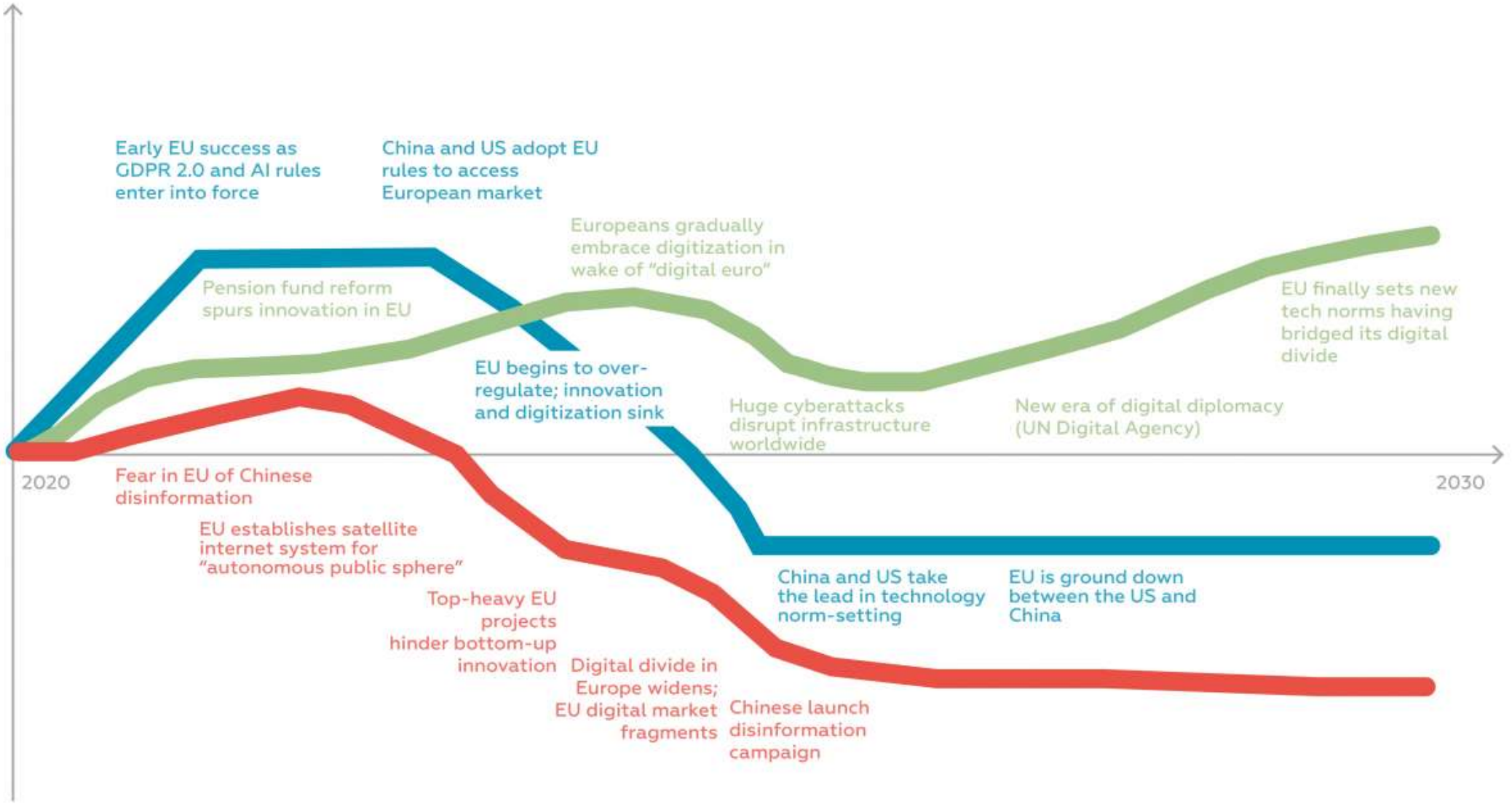
Problems?



Source: United Nations Conference on Trade and Development

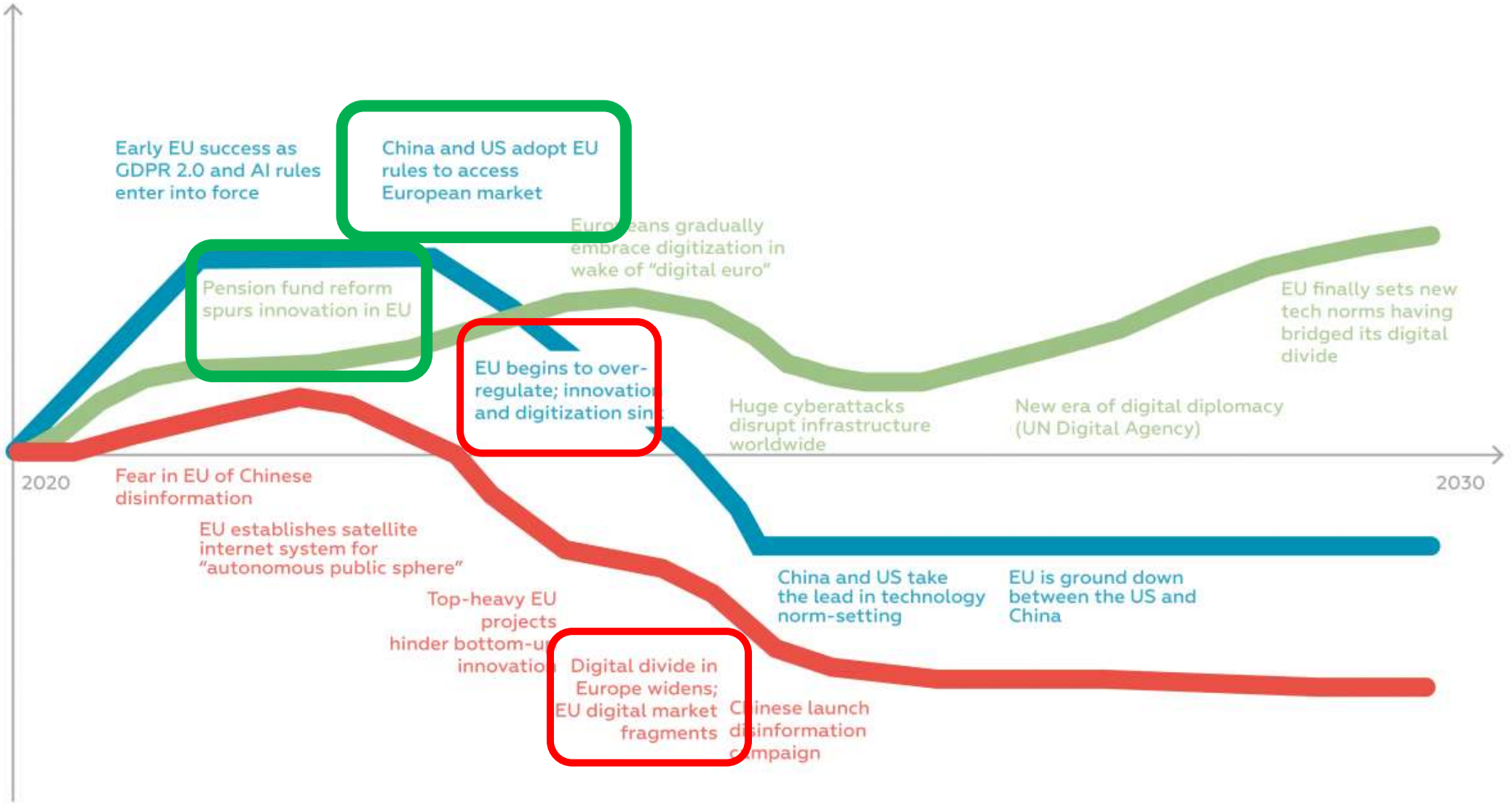
Atlantic Council

1. OVERVIEW OF THE TECHNOLOGY SCENARIOS



DGAP

1. OVERVIEW OF THE TECHNOLOGY SCENARIOS



DGAP

Problems?

- Sovereignty may not be achievable only through better laws
- Low innovation, lack of competition, low investment in next-gen not problems for which sovereignty is the solution

Alternatives

- Resilience
- Capacity to act