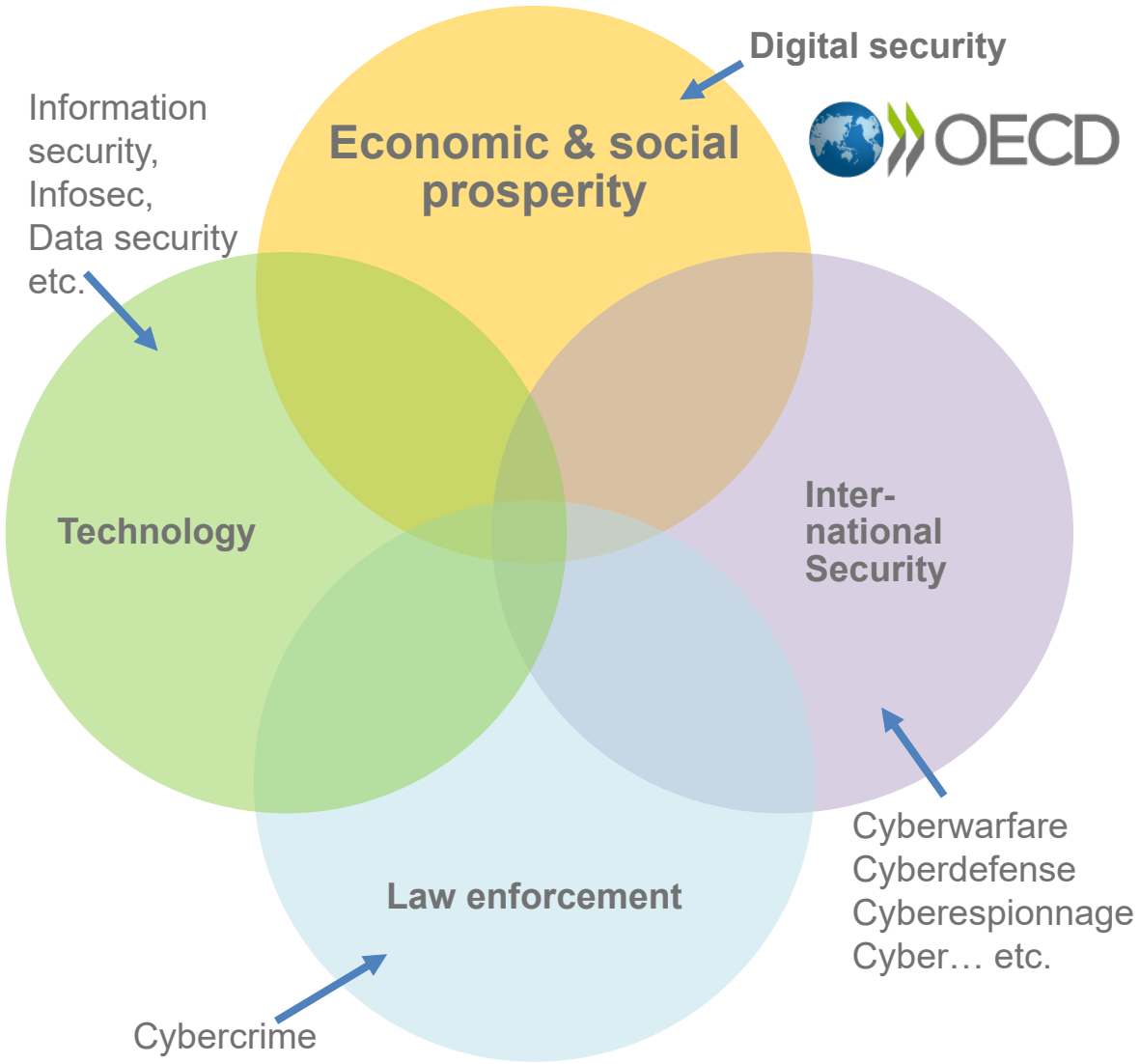
OECD Global Parliamentary Network
Building a secure and inclusive digital future in a post-COVID world
Saeima of the Republic of Latvia, Jēkaba iela 11, Rīga
1 July 2022

OECD WORK ON DIGITAL SECURITY POLICY

BETTER POLICIES FOR BETTER LIVES

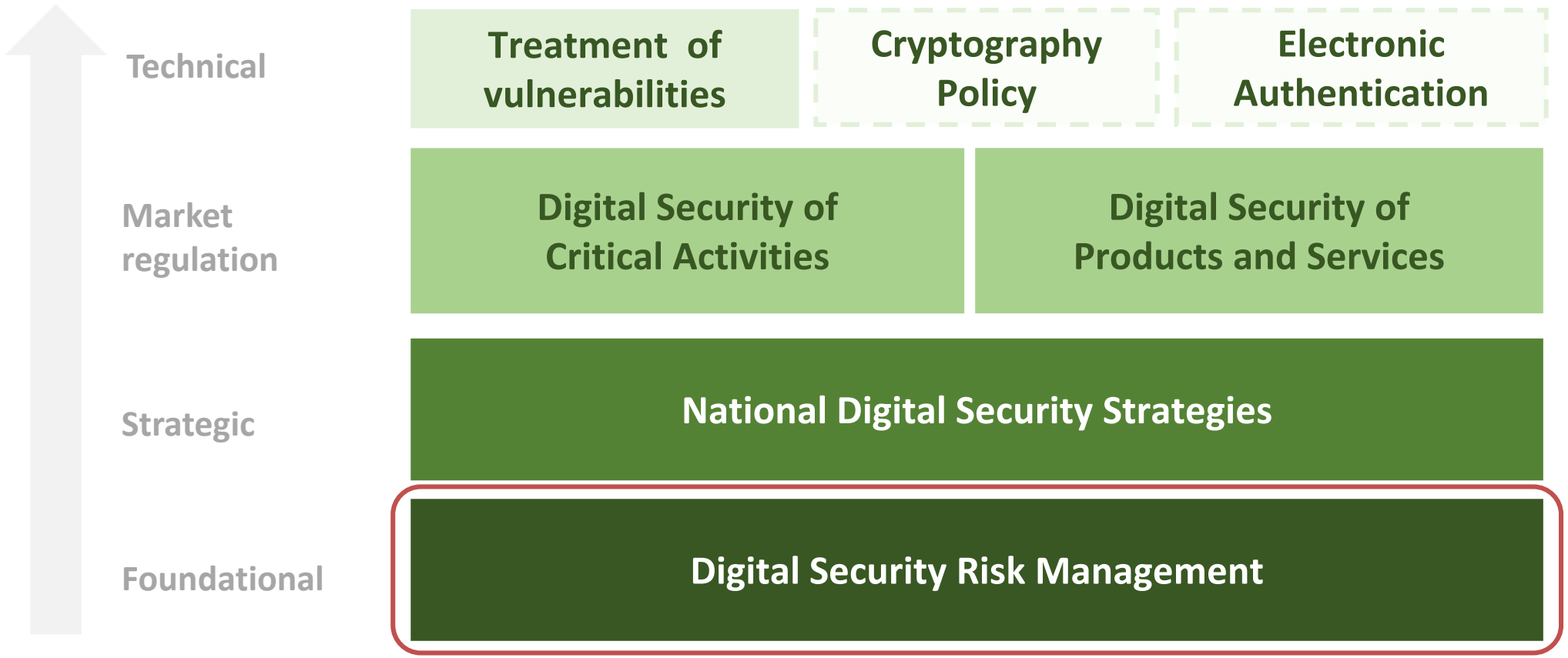
Digital security is an economic and social challenge



- **Why « Digital » and not « Cyber » security ?**
  - Because digital security risk is economic and social
    - « Digital » has economic connotations (e.g. *digital* technologies, economy, transformation… and security)
    - « Cyber » has sovereignty connotations (cyber warfare, cyber espionnage, cyber defence, etc.)

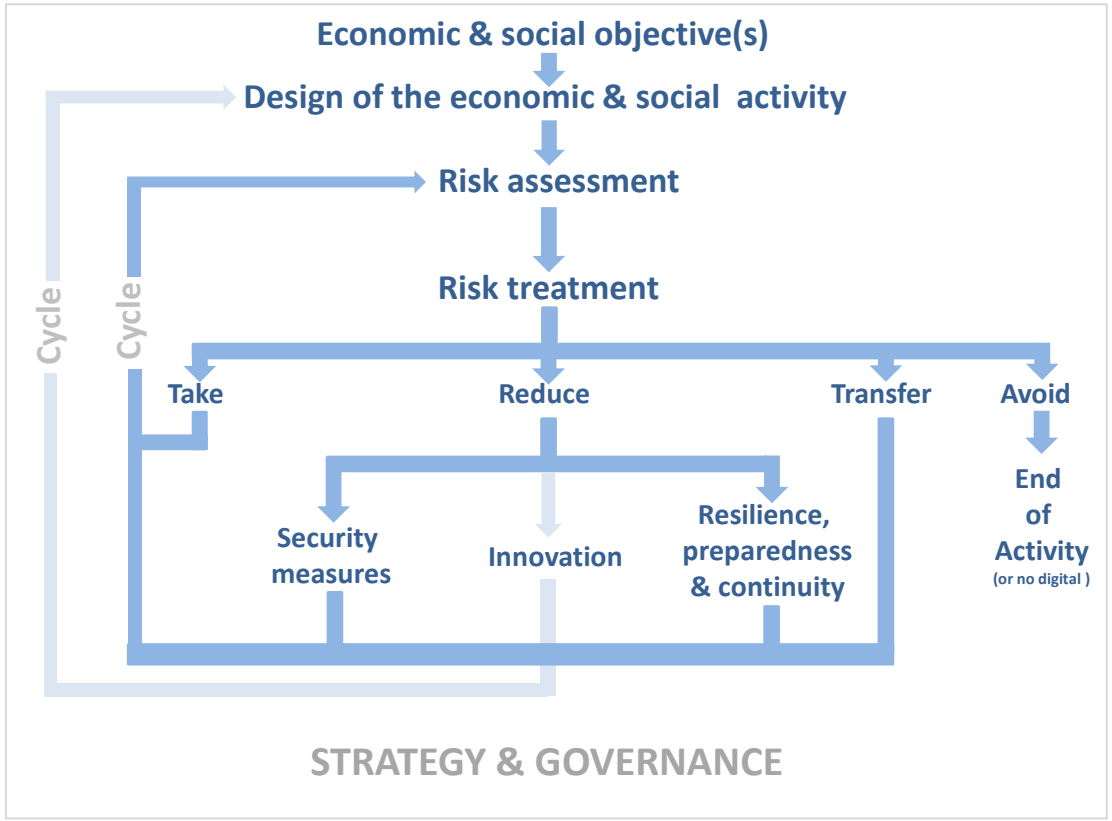
- **Working Party on Security in the Digital Economy (SDE)**
  - Promotes an **economic and social risk management** approach to digital security
  - Builds on nearly 40 years of OECD expertise on digital security, privacy and trust
  - Gathers the community of digital security policy makers focusing on economic and social aspects
  - Reports to the OECD Committee on Digital Economy Policy (CDEP)

Overview of OECD Instruments on Digital Security

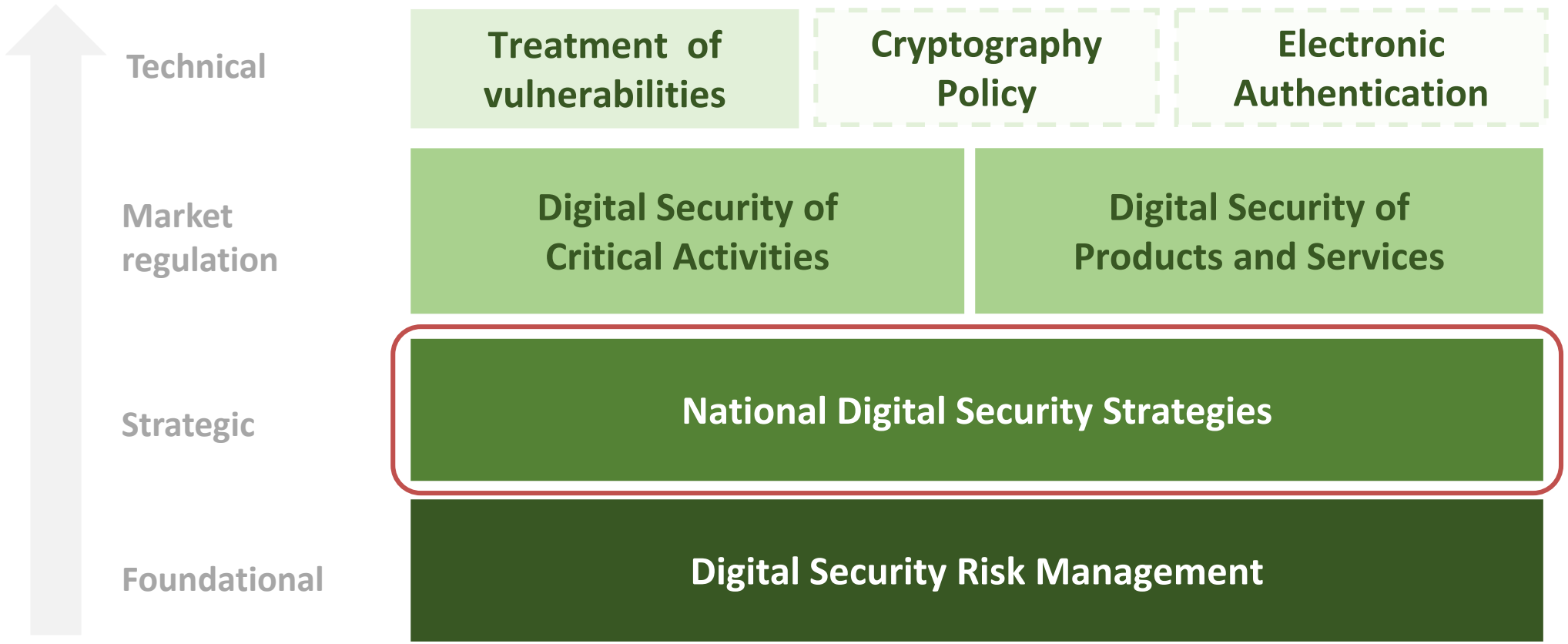


Foundational layer: Digital Security Risk Management

- What is digital security ?
  - Digital security as the economic and social dimension of cybersecurity
  - Digital security fundamentals, e.g.
    - AIC
    - Threats, vulnerabilities, incidents
    - **Economic & social vs technical risk**
- Risk management principles



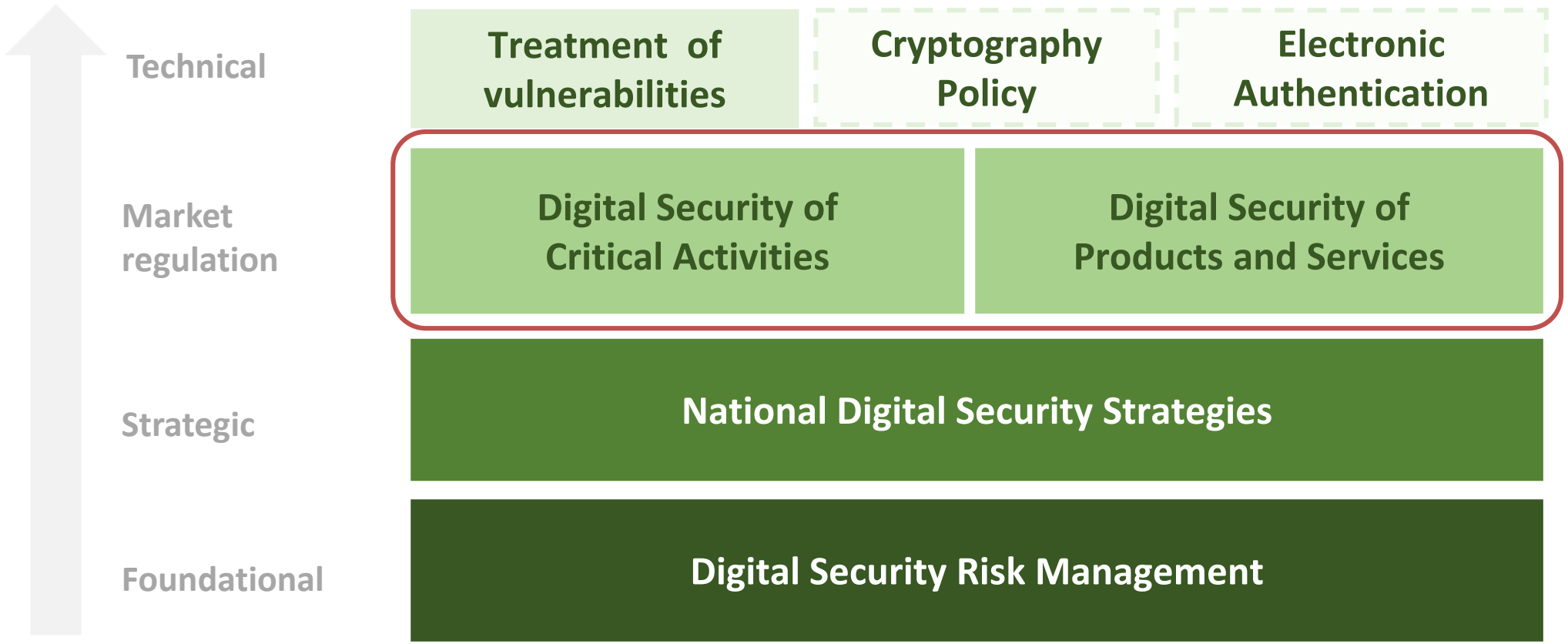
Overview of OECD Instruments on Digital Security



Strategic layer: National digital security strategies setting institutional framework to manage digital security risks

- **Enhanced governmental co-ordination at policy and operational levels:** Responsibility for cybersecurity policy making and implementation is being clearly assigned within the government.
- **Reinforced public-private co-operation:** Recognising that cyberspace is largely owned and operated by the private sector and that users also play a key role.
- **Improved international co-operation:** Reflecting the need for better alliances and partnerships with like-minded countries or allies, including facilitating capacity building of less developed countries.
- **Respect for fundamental values:** Strong emphasis on the need for cybersecurity policy to respect fundamental values, which generally include privacy, freedom of speech, and the free flow of information.

Overview of OECD Instruments on Digital Security



Market level: Strengthening digital security without inhibiting prosperity

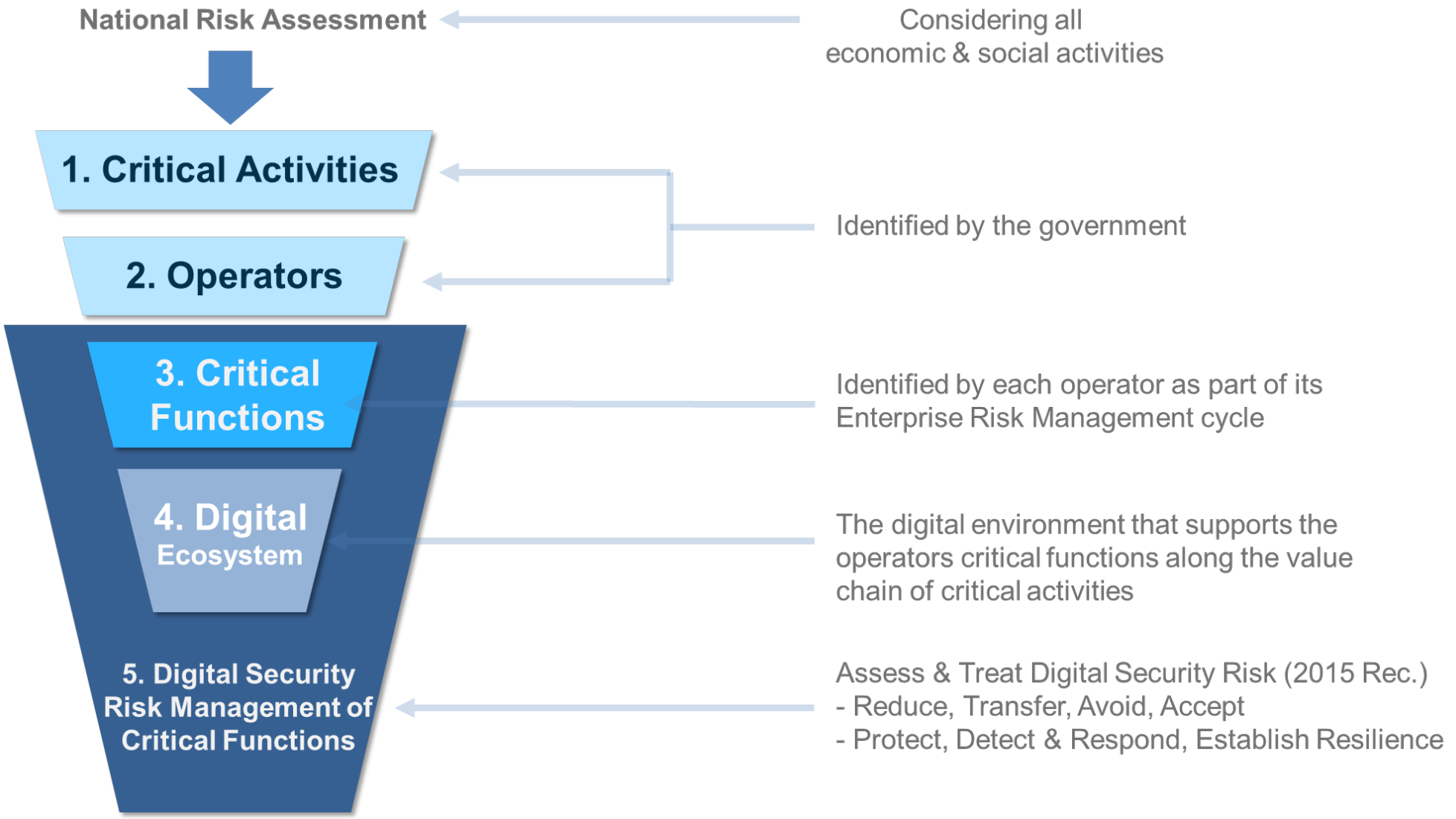
- Stakeholders should take responsibility for managing digital security risks according to their role and abilities.
- However, actors may manage digital security risks in such a way that reduces these risks to the level **they deem acceptable to them**, **but not necessarily to society.**

➢ The economic and social consequences of incidents can extend far beyond these actors and can be catastrophic for all.

➢ **Moral hazard** (externality of risks): “any situation in which one person makes the decision about how much risk to take, while someone else bears the cost if things go badly” (Krugman, 2009)

➢ **How to address this moral hazard to enhance digital security without slowing down innovation and reducing the benefits of digitalisation?**

Digital security of critical activities: Funnelling process



Digital security of products: Why is it important?

With the digital transformation:

- **Code is everywhere**: more and more products are becoming **"smart", i.e. contain code** and can connect.
- Code almost always contains **vulnerabilities**: on average, 40 new vulnerabilities are discovered every day in widely used products such as Windows, iOS and Android.
- **Our digital-dependency** on smart products is increasing, as highlighted by the **COVID-19** pandemic**.**
- As a result, the **impact** of digital security attacks leveraging vulnerabilities in products is increasing significantly.

=> Digital (in)security of products made the headlines in recent years:

- In **2016**, the **Mirai** botnet infected millions of "insecure-by-design" **IoT devices**, enabling massive DDoS attacks.
- In **2017**, **WannaCry and NotPetya** exploited vulnerabilities in unpatched Windows **operating systems**, leading to billions USD in damages.
- In **2018**, **Meltdown and Spectre** vulnerabilities were found in **microprocessors**: "systemic" vulnerabilities?

=> What are the main factors (technical and economic) that explain this situation, and what levers can policy makers use to enhance digital security of products?

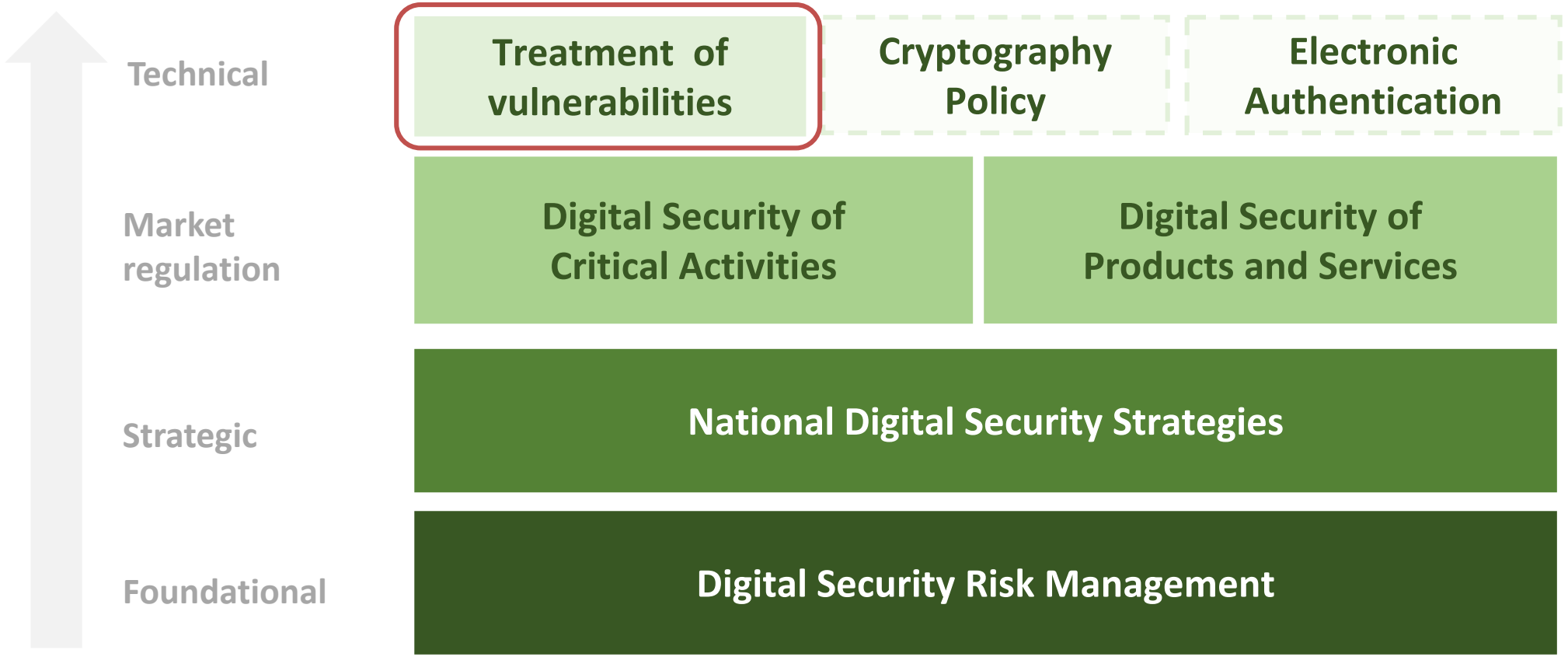
Economic factors play a key role in the digital security of products

- **Misaligned market incentives**: time-to-market, cost effectiveness are often prioritized over security.
- **Information asymmetries:** customers cannot assess the level of digital security of smart products.
- **Negative externalities:** unsecure products impact third-parties and society (e.g. DDoS attacks and botnets).
- **Complex and global value chains** make it difficult to allocate responsibility**.**
- **No "absolute" security**: we cannot achieve 100% security, and it has to be balanced with other objectives.

=>This leads to market failure, i.e. market dynamics on their own are unlikely to deliver an optimal level of cyber security in smart products.

The OECD published two reports in February 2021

Overview of OECD Instruments on Digital Security



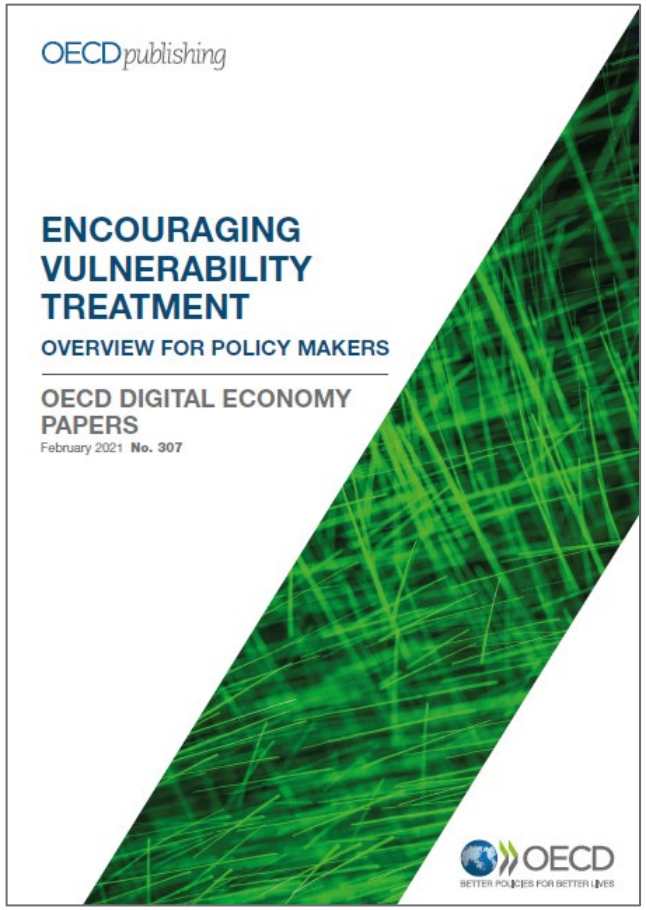
Technical layer: Common misconceptions of vulnerabilities - a more complex area than it appears

We thought that…		When in fact…
This is only about zero-days	➔	Need to consider code and system vulnerabilities
This is only about coordinated vulnerability disclosure (CVD)	➔	Need for a holistic approach, hence vulnerability treatment
Bug bounty is a silver bullet	➔	One tool among others
This is a technical problem	➔	Obstacles are economic (grey market, incentives), legal (safe harbours), cultural (vulnerability taboo).
Government is always neutral	➔	Trust in government can be a challenge

Key findings for policy makers

- **Not all vulnerabilities are equal**
  - Code vs system vulnerabilities
  - Severity vs risk
- **Vulnerabilities are a fact of digital life**
  - It is not possible to eradicate them
  - But treating them is a key opportunity to reduce risk for all
- **Significant economic and social challenges prevent stakeholders from treating vulnerabilities effectively**
  - Not only a technical issue
  - Legal risk to security researchers is a significant obstacle

OECD analytical work on vulnerabilities



Report

Policy Note

Looking for more information ?

Check our website:
https://oe.cd/security

Contact the OECD Secretariat:
digitalsecurity@oecd.org

Thank you!