Critical Energy Infrastructure

Resilience of Critical Infrastructure

Professor : **Nasi Greta**
Academic Year : **2022 / 2023**

POLITECNICO
MILANO 1863

Campo Marco Lorenzo - 103213
Grazioli Davide – 992467
Santomauro Carmine - 995752
Savino Matteo - 994779

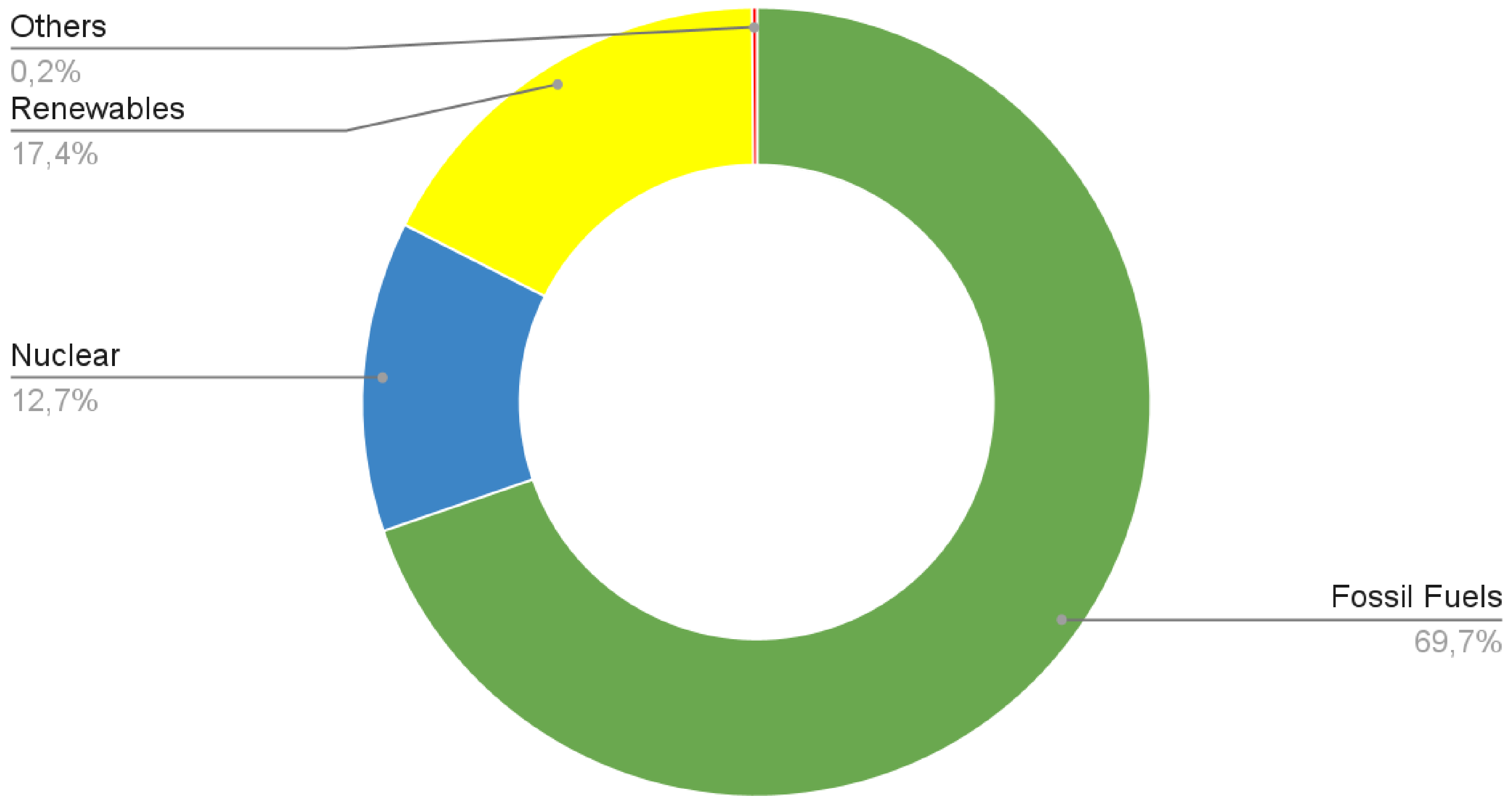
INDEX

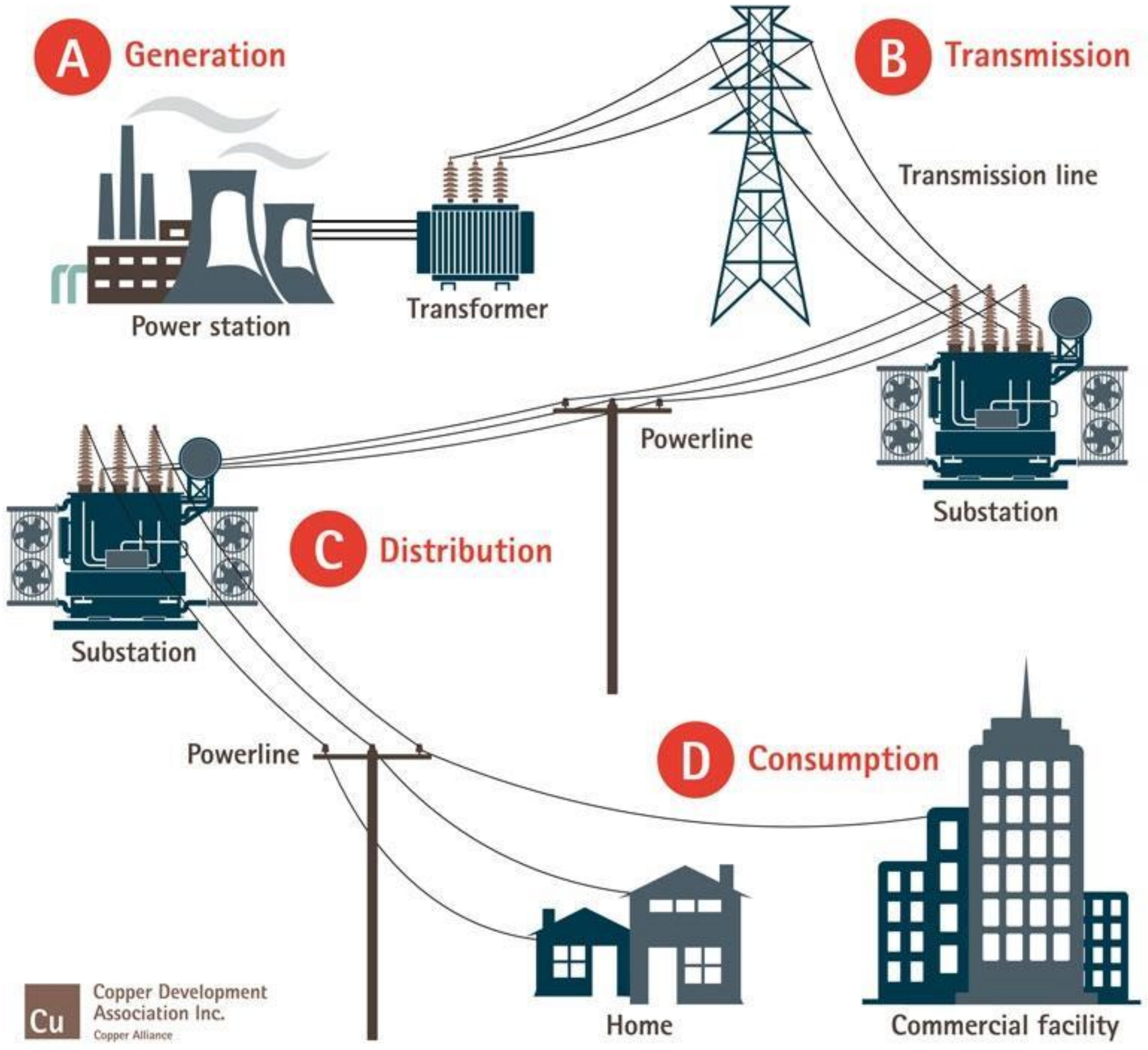
1. Key Characteristics of the CEI (Critical Energy Infrastructure)

KEY CHARACTERISTICS

- Power Stations
  - Fossil Fuels
  - Nuclear
  - Renewables
- Transmission Lines
- Control Centers

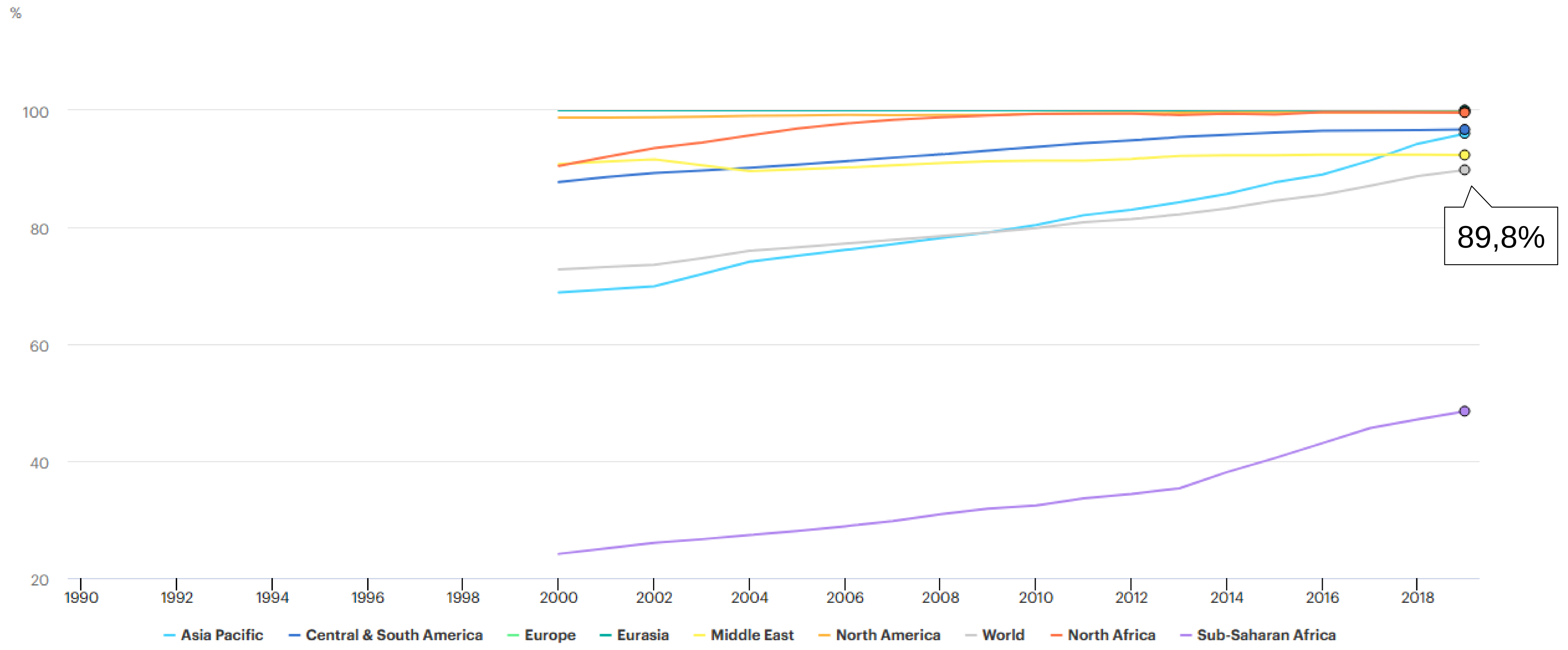
Electricity generation by source, Europe 2020 (europa.eu)





RELEVANCE

Share of population with access to electricity



89,8%

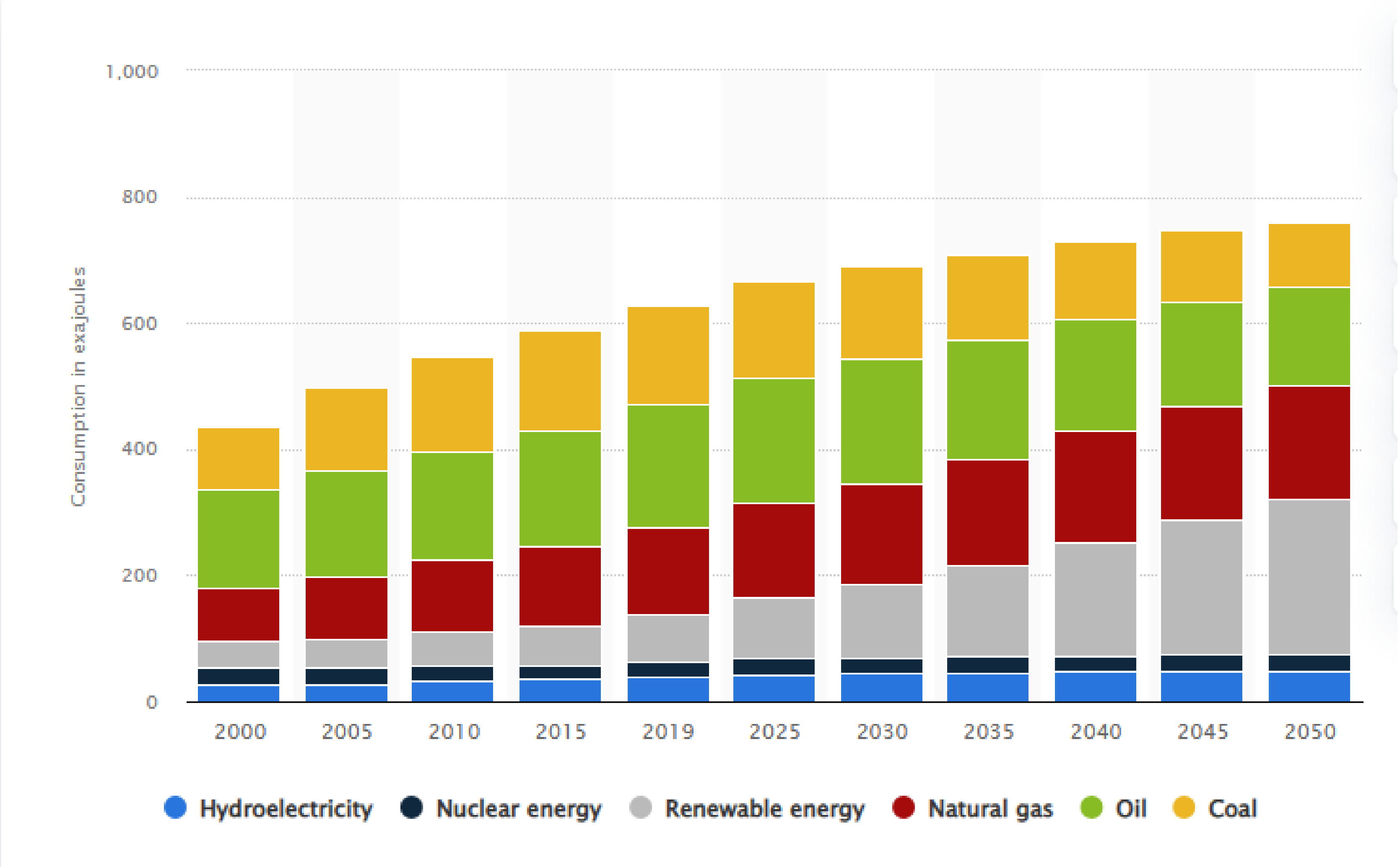
IEA. All Rights Reserved

Sources

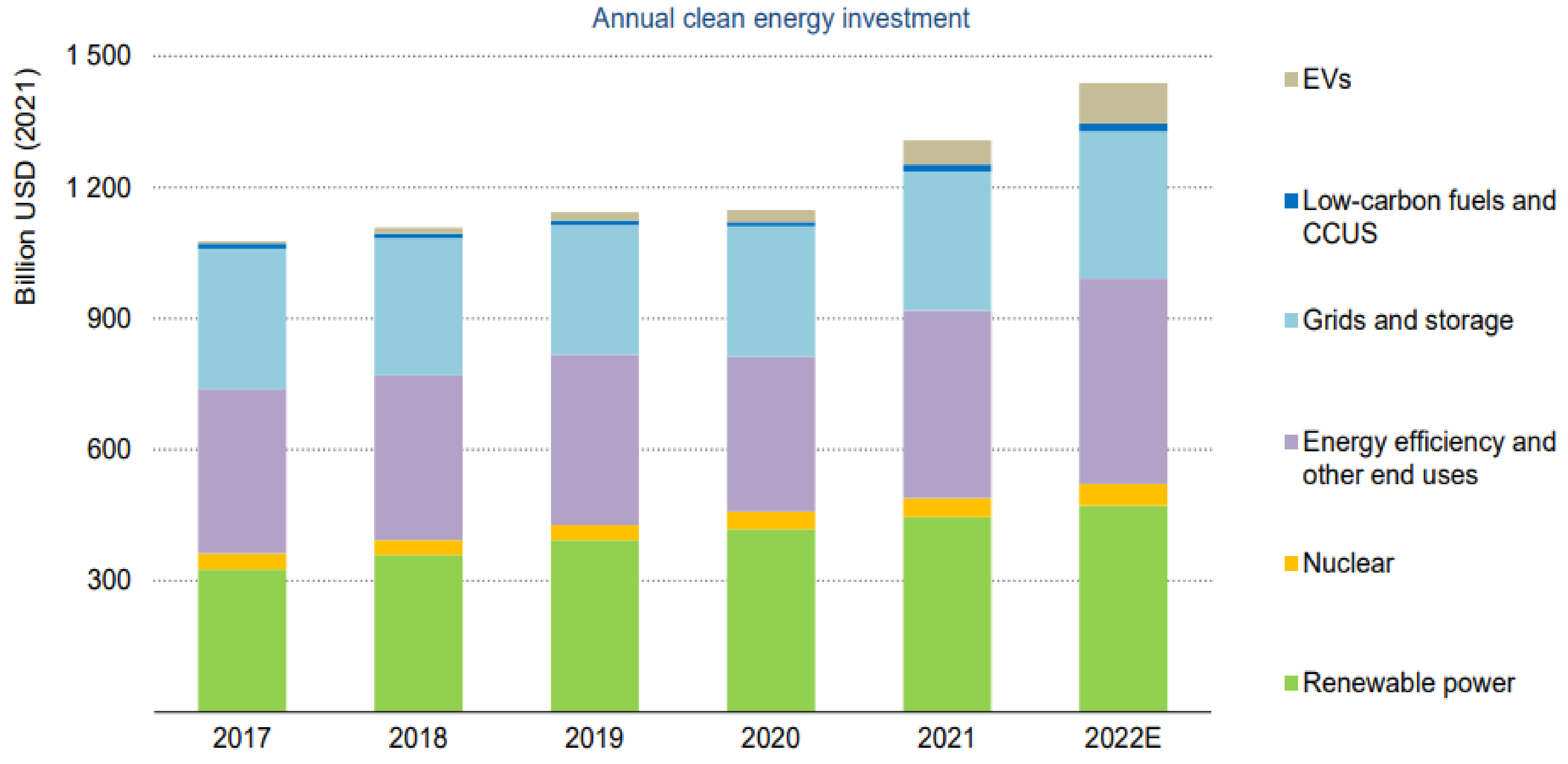
IEA produces its own estimates for access to electricity based on administrative data collected from Ministries of Energy. This data may differ from what is reported by the World Bank in the Tracking SDG7 Report, which uses survey data.

TRENDS

Energy consumption has risen steadily from 2000 to the present, and studies indicate that this increase will continue in the future.



Investments in the energy market in recent years have focused on carbon-free production sources and storage and transportation efficiency



Prof : **Nasi Greta**
AY: **2022 / 2023**

INTERDEPENDENCIES WITH OTHER INFRASTRUCTURES

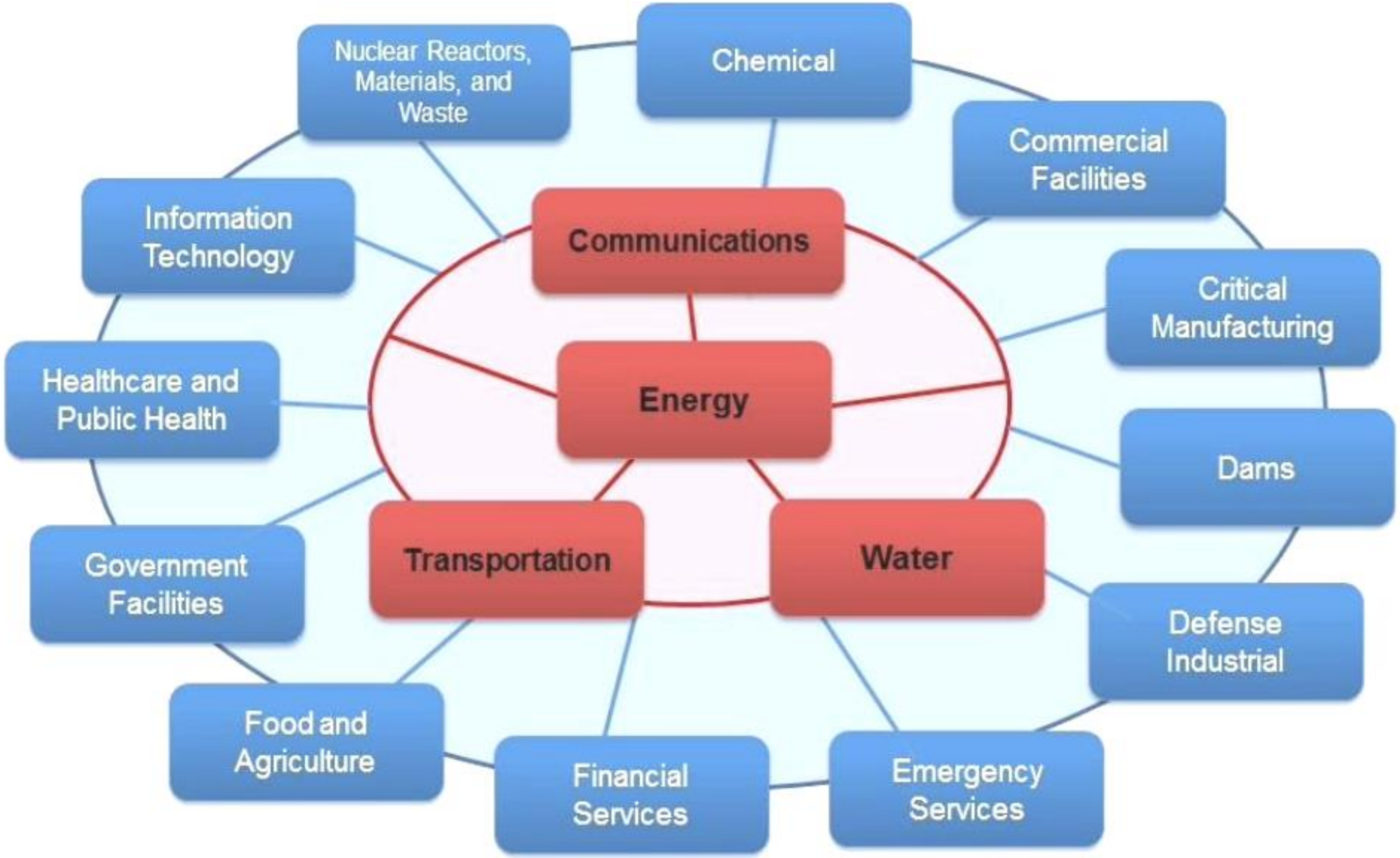
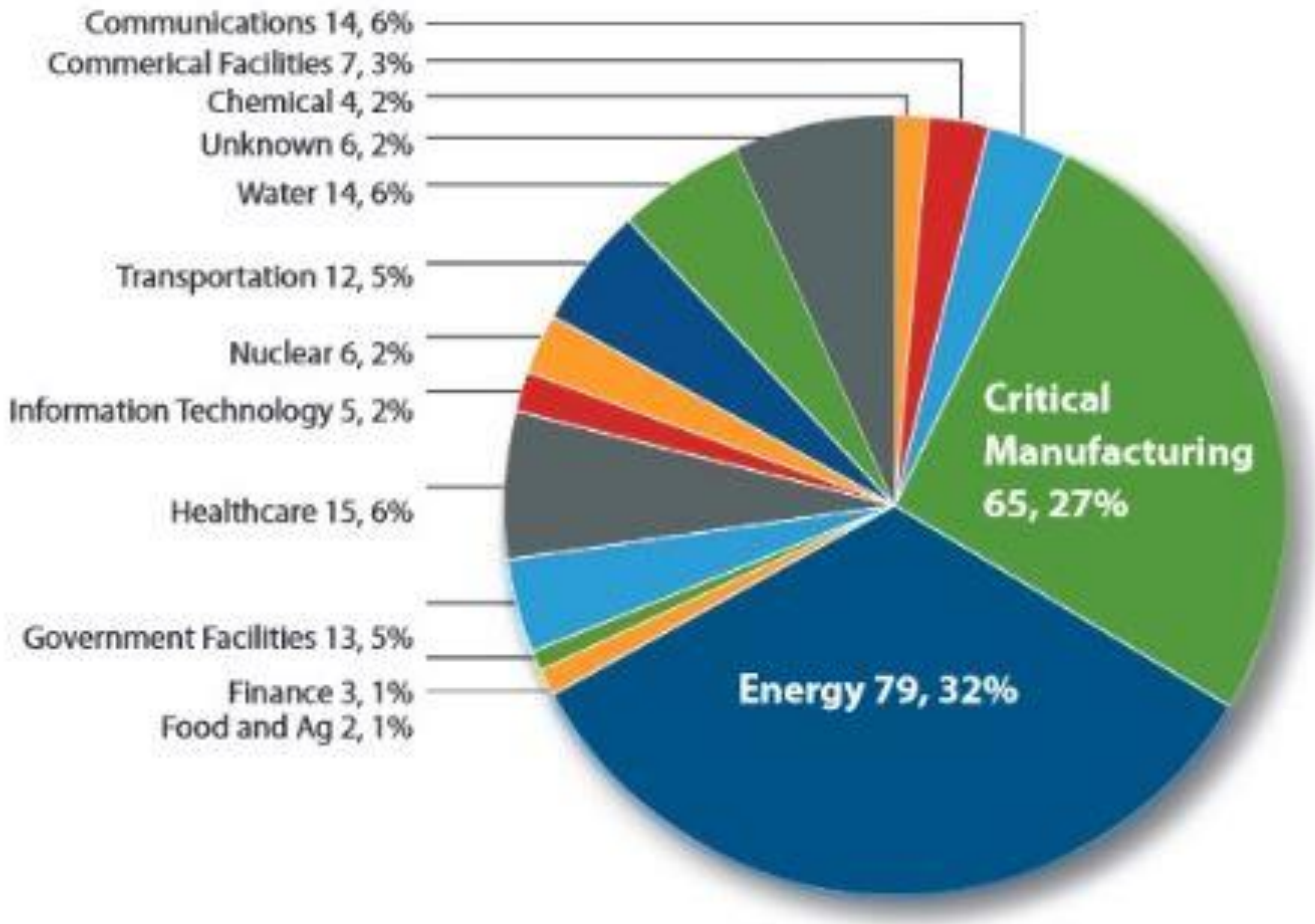


Figure 3: Critical Infrastructure Interdependencies

MAIN KNOWN ATTACKS

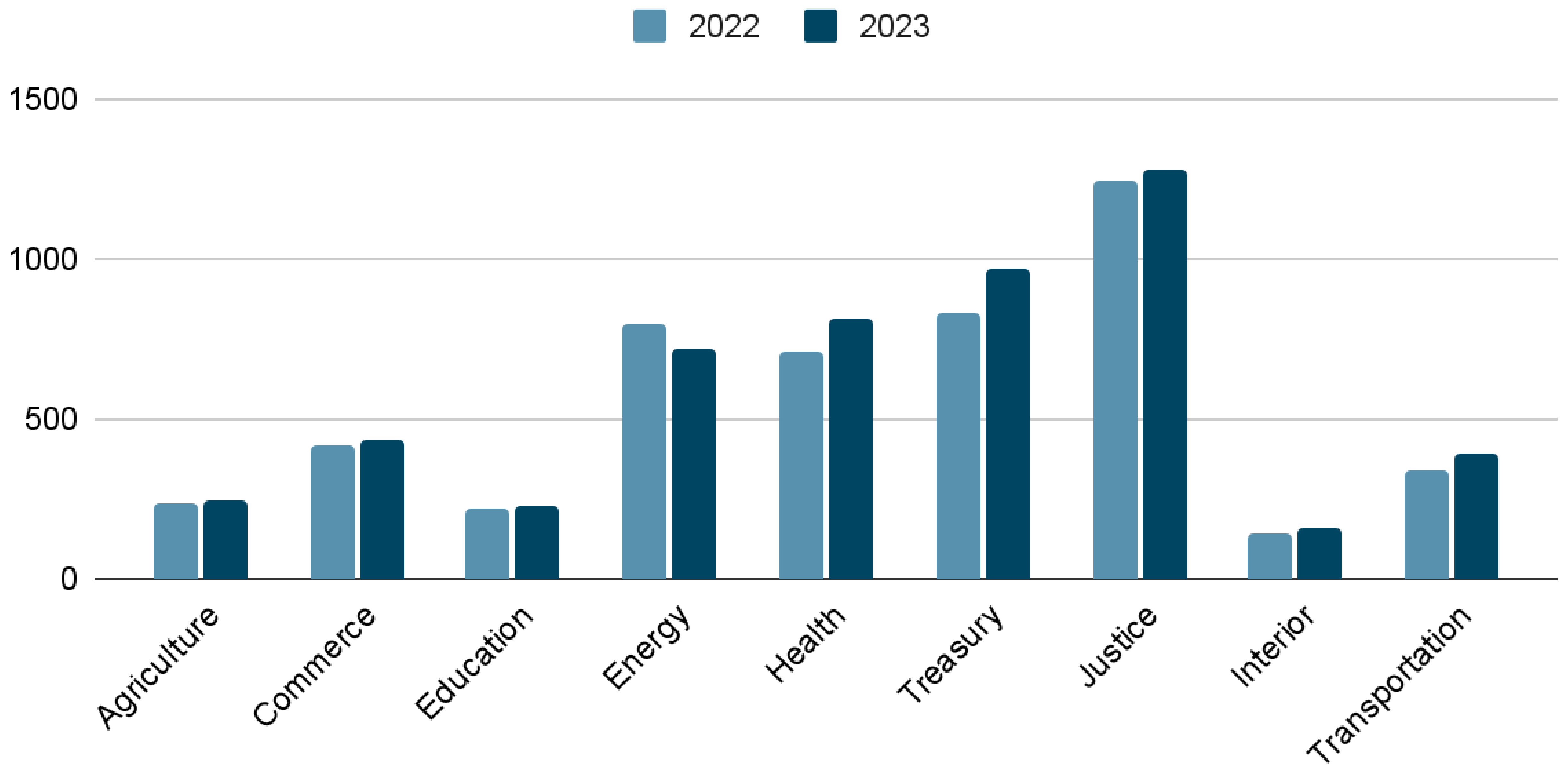
- Ukraine Power Grid Attack (2015)
- NordStream2 Attack (2022)



Incidents of Cyber Attacks in US in 2015

WHAT IS AT RISK?

- Critical Infrastructures
- Population
- Environment
- Data
- Reputation



spending by the U.S. federal government on cybersecurity per department (in milion of dollars)

2. Regulative Frameworks

Stakeholders, Objectives, Risk Assessments, ISO Standards

EU STRATEGY FOR RESILIENCE

From the *European Commission Press release* of 18/2/2022:
critical infrastructures need to be improved in three priority areas:

- **Preparedness**
- **Response**
- **International cooperation.**

Envisioning increased stakeholder support and coordination.
The Critical Energy Infrastructure is perceived as a priority.

STAKEHOLDERS INVOLVEMENT

GOVERNMENT AGENCIES

European Parliament

Council of the European Union

European Commission

REGULATORS

ACER
European Union Agency for the Cooperation
of Energy Regulators

DISTRIBUTORS

Enel Distribuzione

endesa

PRODUCERS

enel

Shell

Involvement of the stakeholders:

- European Stakeholders Committee (ESCs)
- Energy Stakeholders Dialogues

KEY REGULATORY FRAMEWORKS (1/2)

CER Directive (Critical Entities Resilience):

- Repeals the ECID (European Critical Infrastructure Directive) of 2008
- Strengthens the resilience of Critical Infrastructures
- Promotes national strategies for EU members
- Promotes regular risk assessments and reporting

NIS2 Directive (Network and Information Systems):

- Establishment of a cooperation group on cybersecurity
- Establishment of a cybersecurity certification framework
- Expansion of the scope (*cap-size rule*)
- Based on the NIS Directive

KEY REGULATORY FRAMEWORKS (2/2)

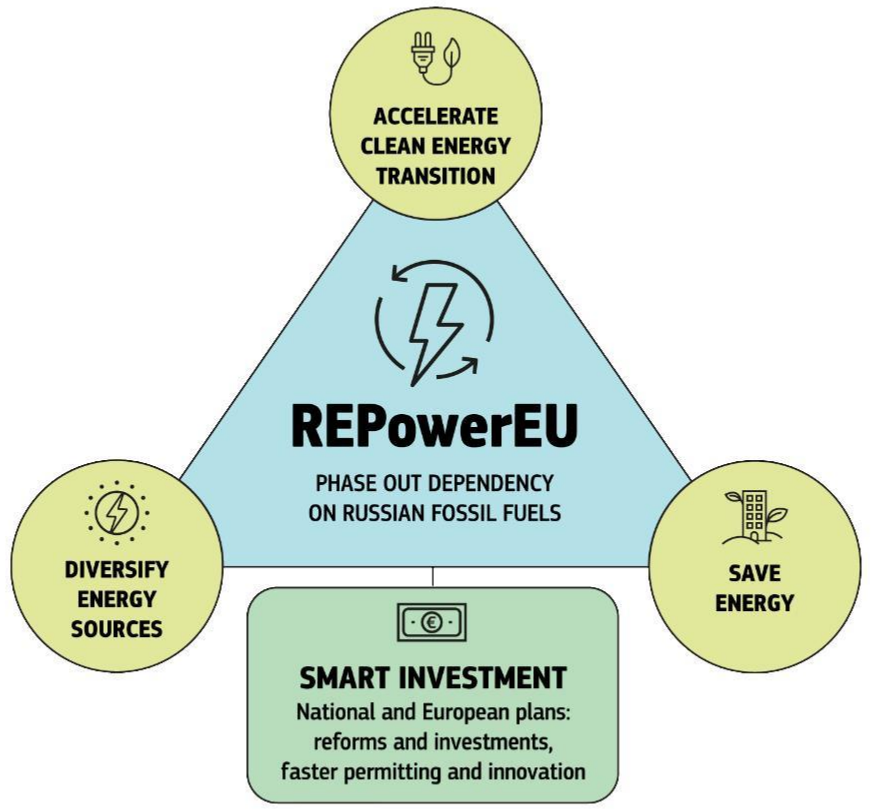
ENISA (European Network and Information Security Agency):

- Development policies, strategies, and frameworks
- Identification and assessment of cyber risks
- Promotion of cybersecurity awareness
- Development of technical standards and certifications
- Promotion of international cooperation and collaboration

TEN-E (Trans-European Networks for Energy):

- Promotion of a cross-border energy infrastructure
- Integration of national energy markets into a single, integrated one
- Wide range of energy infrastructure
- Focus on renewable energy sources

REPowerEU: Energy Independence framework focused on Russian gas, focusing on green energy.



ACCELERATE CLEAN ENERGY TRANSITION

REPowerEU

PHASE OUT DEPENDENCY ON RUSSIAN FOSSIL FUELS

DIVERSIFY ENERGY SOURCES

SMART INVESTMENT

National and European plans: reforms and investments, faster permitting and innovation

SAVE ENERGY

RISK ASSESSMENT MODELS AND ISO STANDARDS

European Union Agency for Cybersecurity **(ENISA) RM/RA** (Risk Management/Risk Assessment) **inventory**.

Final text of the **Critical Entities Resilience Directive (CER)**:

- Article 5, Risk assessment by Member States, CER Directive.
- Article 12, Risk assessment by Critical Entities, CER Directive.

International Organization for Standardization

Employed ISO Standards:
ISO 14001: environmental management systems
ISO 50001: energy management systems
ISO 55001: asset management

3. Assets and Vulnerabilities

ASSETS

- **Energy Production:**

Power plants: fossil fuel power plants, nuclear power plants, wind farms, solar power plants etc

- **Energy Distribution and Transportation:**

Transmission and distribution networks: High voltage transmission lines, transformers and substations
Oil and gas pipelines: transport from production to refineries and end users

- **Energy Storing:**

Fuel storage facilities: storage tanks for oil and gas
Energy storage facilities: batteries, pumped hydroelectric storage

- **Energy Control Systems**

Energy control systems: this include the computer systems and software used to manage energy production and distribution

VULNERABILITIES

- **Aging Infrastructure:** if we take the US as example, 70% of transmission lines are at least 25 years old and 60% of circuit breakers are more than 30 years old. Aging infrastructure increases the risk of equipment failure, which can result in outages or other disruptions.
- **Aging Workforce:** Human Factor is always a vulnerability. However, the growing potential gap in available skilled personnel to replace the retiring workforce has been a real concern in the Energy Sector for some time. Retiring people take years of experience with them and it is crucial to train new generation of skill workers.
- **Dependance on Limited Resources:** heavily relying on stock-limited resources such as fossil fuels (coal, petroleum, natural gas) which are not equally available to every nation

THREATS

- **Cyberattacks**: As the energy sector relies heavily on technology and the internet, it is vulnerable to cyberattacks.
- **Physical Attacks**: The energy sector's physical infrastructure, such as power plants and pipelines, is also vulnerable to physical attacks
- **Natural Disasters**: The energy sector is also vulnerable to natural disasters, such as hurricanes, earthquakes, and wildfires, which can damage infrastructure and disrupt energy supplies.
- **Geopolitical Risks**: The energy sector is often affected by geopolitical risks, including political instability, war, and sanctions, which can disrupt energy supplies and increase prices.

RELIABLE DATA SOURCES

- **IEA(International energy agency)**: The IEA is at the heart of global dialogue on energy, providing authoritative analysis, data, policy recommendations, and real-world solutions to help countries provide secure and sustainable energy for all.

- **ENISA(European Network and Information Security Agency)**: focuses on improving cybersecurity across all sectors in the EU and produces reports and provides guidance on best practices for securing energy infrastructure.

- **IRENA(International renewable energy agency)**: The International Renewable Energy Agency (IRENA) is a lead global intergovernmental agency for energy transformation that serves as the principal platform for international cooperation, supports countries in their energy transitions, and provides state of the art data and analyses on technology, innovation, policy, finance and investment.

- **Eurostat**: Eurostat is the statistical office of the European Union and provides a wide range of statistics on energy, including production, consumption, and renewable energy sources.

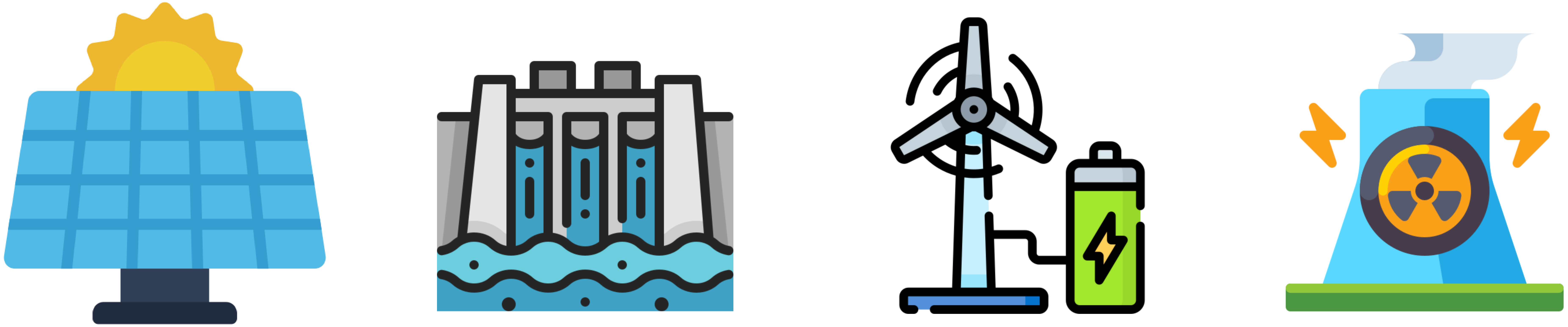
4. Recommendations for the CI

SECURITY AND RESILIENCY

- **Diversify** energy sources, suppliers and routes.
- Create a deeper **collaboration** plan between EU countries at an international level.
- Invest in **energy storage** technologies.
- Adapt/Substitute **legacy systems** and invest in automated threats detection tools.

SUSTAINABILITY AND GREEN

- Improve energy **efficiency**
- Increase investment in **renewable energy** sources



DO NOT FORGET STAKEHOLDERS!

As we have previously highlighted, there are multiple stakeholders in the Energy Critical Infrastructure:

- **Companies**
- **Governments**
- **Regulators / Policy Makers**
- **Consumers**
- **More stakeholders** (e.g. Investors, Local Communities)

Their interests and concerns must all be considered while creating new policies, even though they have a very diverse point of view.

Thank you!

POLITECNICO
MILANO 1863

Campo Marco Lorenzo - 103213

Grazioli Davide – 992467

Santomauro Carmine - 995752

Savino Matteo - 994779

Prof : **Nasi Greta**
AY: **2022 / 2023**

RESOURCES

- Critical infrastructure and cybersecurity (europa.eu)
- Cyber-Incidents in the Energy Sector - Ecofys
- CEI Security Stakeholder Group Manifest
- National Infrastructure Protection Plan - Department of Energy - Homeland Security
- Where does our energy come from? (europa.eu)
- World Energy Investment 2022 - IEA
- Access to electricity – SDG7: Data and Projections – Analysis - IEA
- Energy consumption by source - Statista
- Energy sector tops list of US industries under cyber attack - Homeland Security report
- Cybersecurity Special: Energy industry cyberattack target number one (hornetsecurity.com)
- U.S. government cybersecurity spending FY 2023 - Statista
- The Critical Entities Resilience Directive (CER)
- Critical Infrastructure Resilience: stronger rules
- Critical Infrastructure: Commission accelerates work to build up European resilience
- Energy security
- Critical Infrastructure Resilience: stronger rules
- Energy security
- METHODOLOGY FOR SECTORAL CYBERSECURITY ASSESSMENTS
- Critical infrastructure and cybersecurity
- Energy storage
- Digitalization set to transform global energy system with profound implications for all energy actors - News - IEA
- Ukrainian experience | building cyber resilience - KPMG Ukraine
- Accelerating energy efficiency: What governments can do now to deliver energy savings – Analysis - IEA
- REGULATION AND STANDARDS FOR A RESILIENT EUROPEAN ENERGY SYSTEM
- Cyber-attacks to critical energy infrastructure and management issues
- National conference on state legislatures, 2020
- https://www.uscybersecurity.net/csmag/accelerating-critical-infrastructure-security-in-the-energy-sector/
- https://www.iea.org/about/mission
- https://www.irena.org/about
- https://ec.europa.eu/eurostat
- Germany, EU remain heavily dependent on imported fossil fuels | Clean Energy Wire