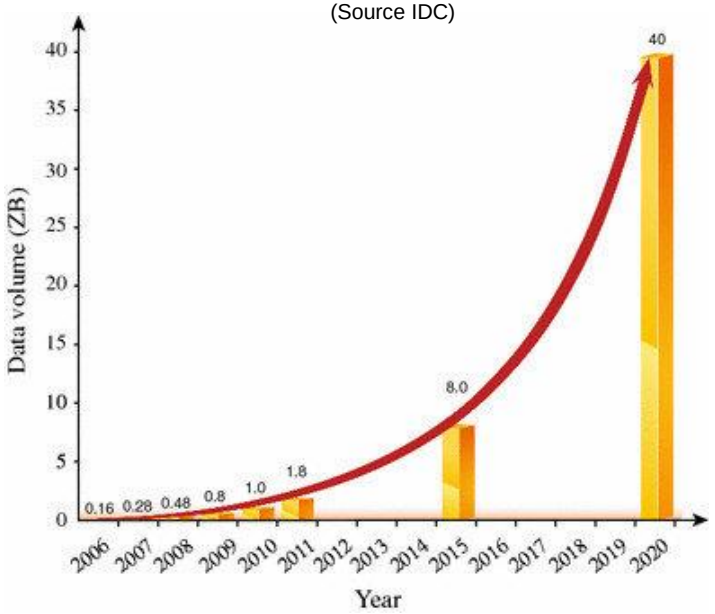
Cybersecurity Policy Making

Giacomo Assenza
06/12/2021

More Data and More Exposed

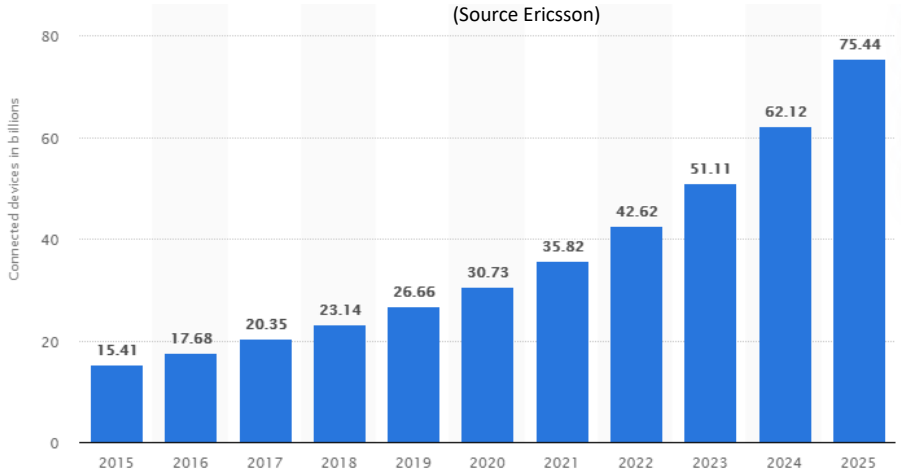
Annual Data Generation per Year

(Source IDC)



IoT connected devices installed base worldwide from 2015 to 2025

(Source Ericsson)



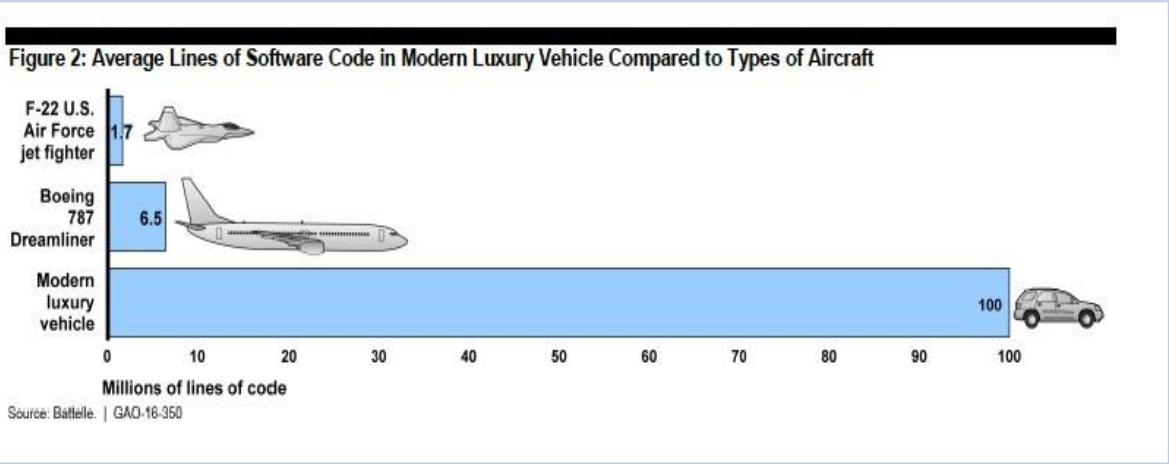
4IR impact on cybersecurity

- Capacity of collecting data
- Capacity of storing and sharing data
- Capacity of analyse and infer

→

- More Vulnerabilities
- Broader attack surface

Cybersecurity and Digital Transformation



Average of 15 – 50 errors per 1000 lines of delivered code

(Code Complete)

<u>4IR Paradigm is all-encompassing</u>

- Production
- Domotics
- Smart cities
- eHealth
- Energy
- Critical Infrastructure
- eCommerce
- IoT
- Banking
- Finance

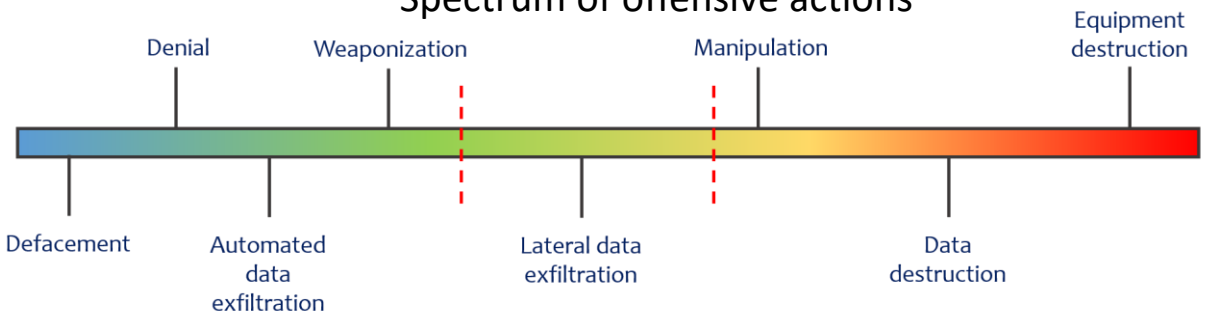
Cybersecurity is a key enabler of digital transformation

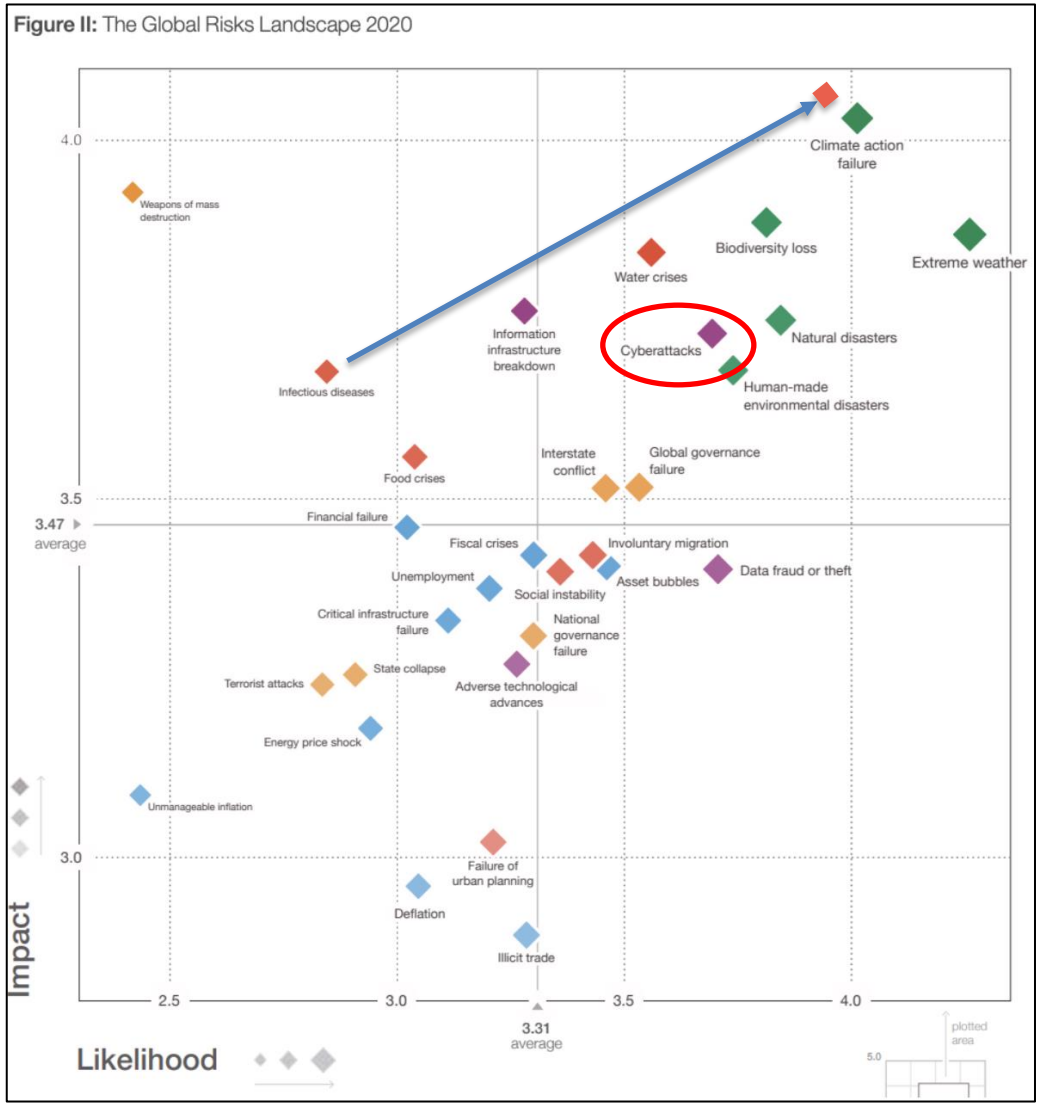
A rapidly increasing number of new cybersecurity risks emerge stressing the need to strengthen cyber resilience:

- Compromising physical security
- Services disruptions
- Personal data
- Production downtimes
- Damaging equipment
- Financial losses
- Reputational losses

In recent years the **Global Risks Report** has identified cyberattacks as very likely to happen with a very high impact: "*Offensive cyber capabilities are developing more rapidly than our ability to deal with hostile incidents*"

Spectrum of offensive actions





Cybersecurity and Digital Transformation

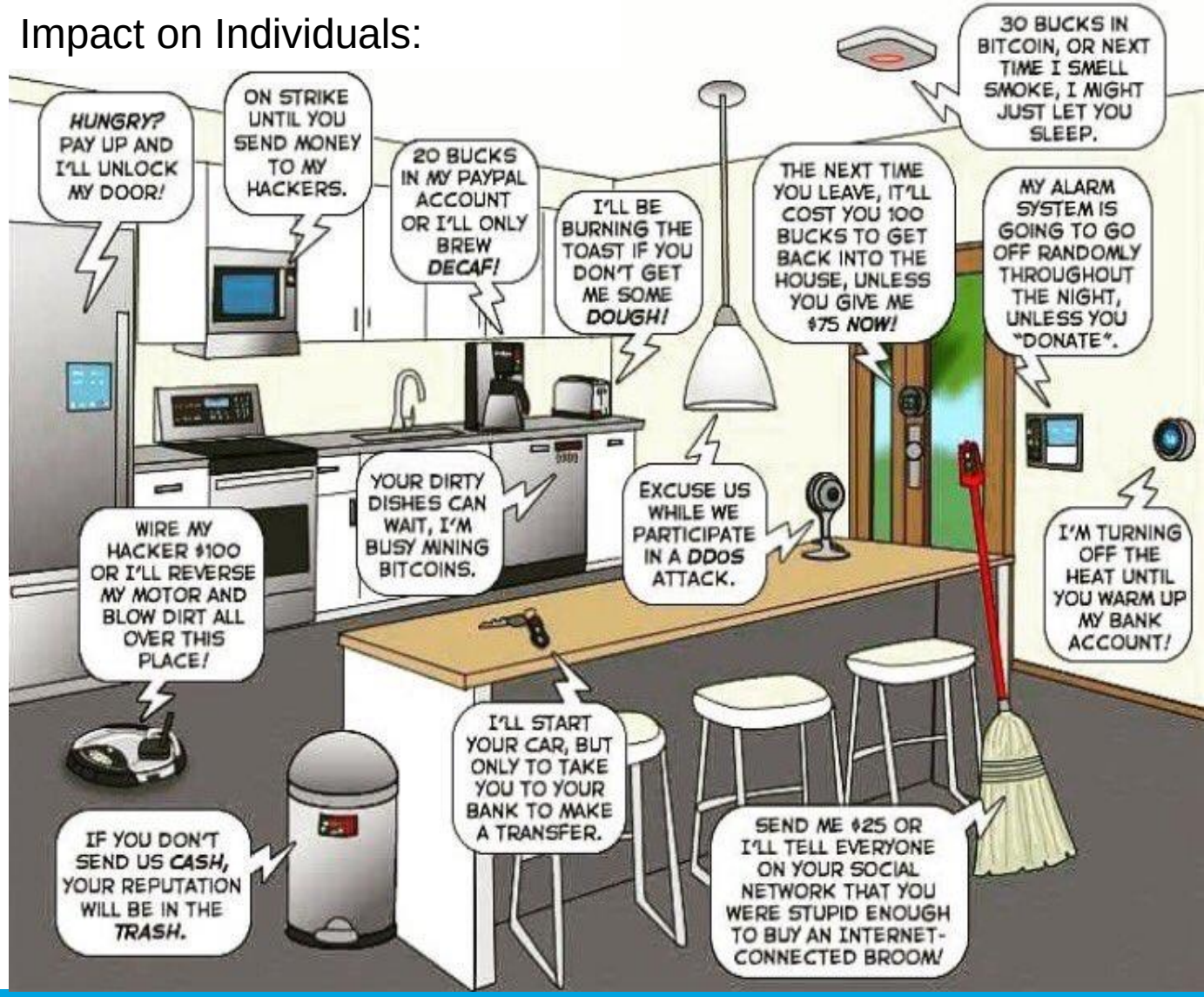
Potential impacts

- **Disruption of operations**
- **Disruption of essential services**
- **Economic impact**
- **Public safety**
- **Theft of data**
- **Intellectual Property theft, etc.**

Cyber risks for all 4IR verticals

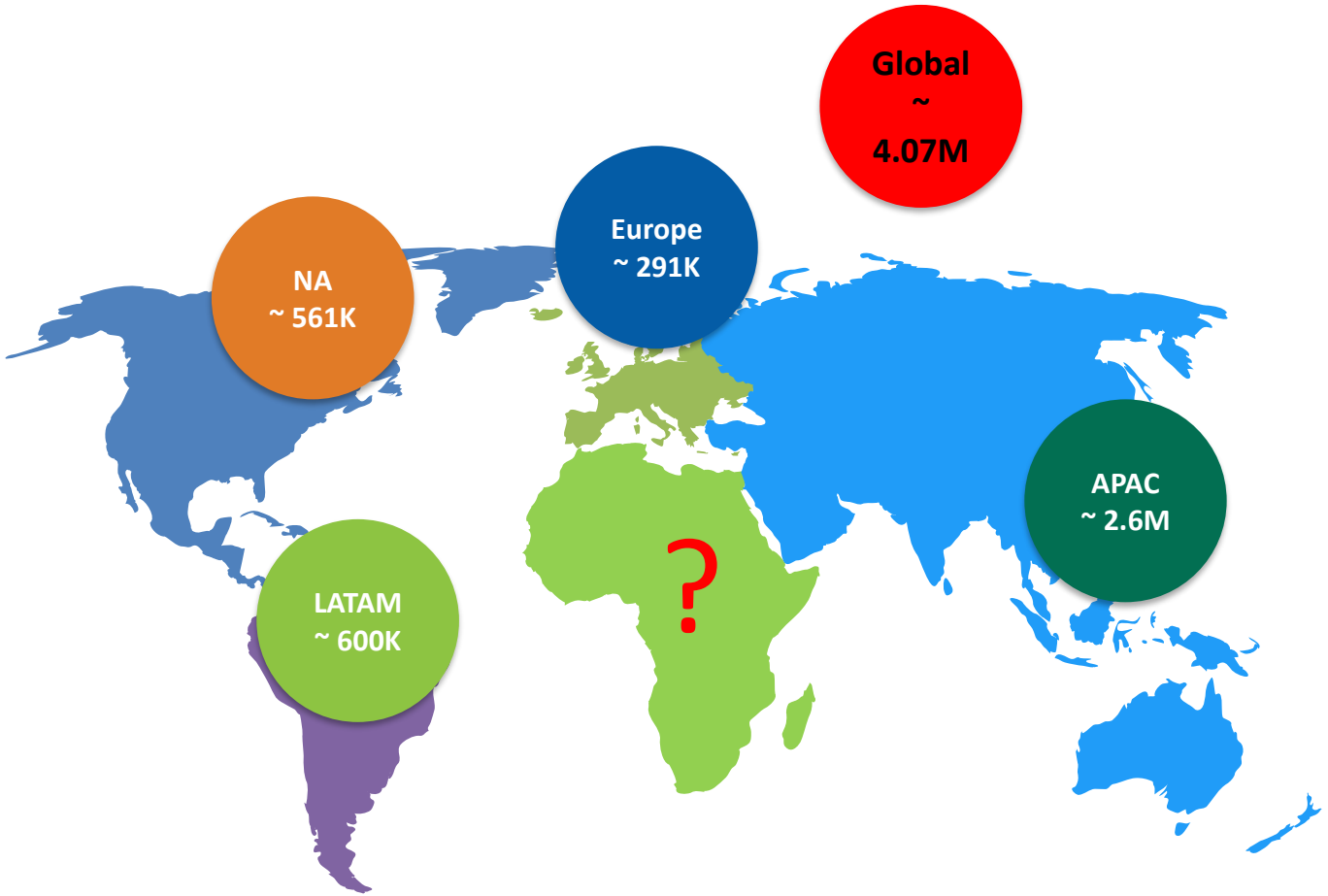
- Smart grids
- Smart roads
- Smart building
- Supply of essential services
- Industry
- Communication
- Healthcare
- Wearable devices
- Bank and Finance
- Smart everything

Impact on Individuals:



The Cybersecurity Workforce Gap by Region

Source: ISC2

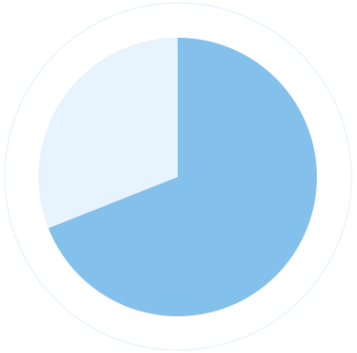


3.5 Million

The number of unfilled cybersecurity positions globally by 2021

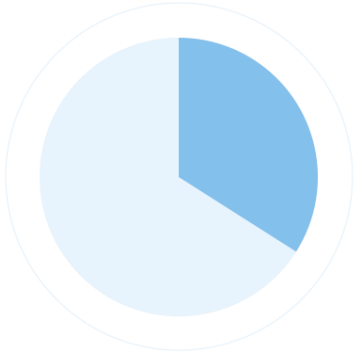
- Cybersecurity Ventures

Cybersecurity Skills Gap



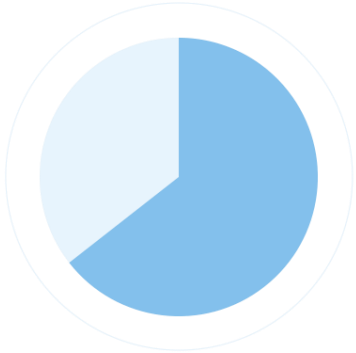
69% of Managers

"Cybersecurity Teams are understaffed"



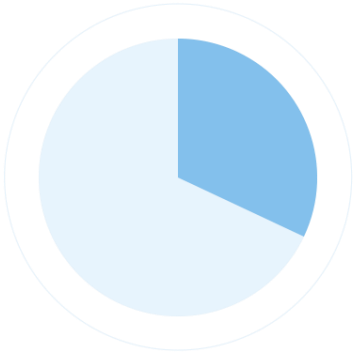
34% of Managers

"Have a high confidence in their team's ability to detect and respond to cyber threats"



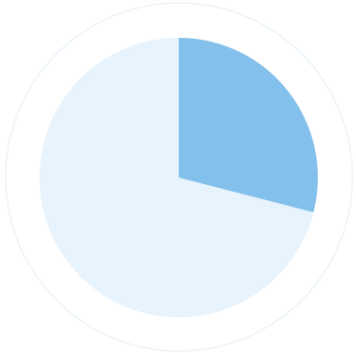
58% of Managers

"Have unfilled cybersecurity positions"



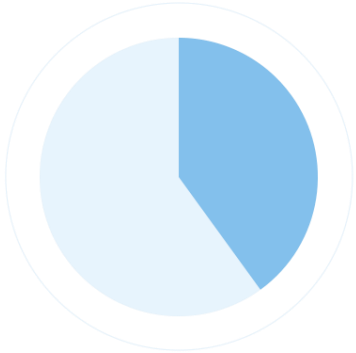
32% of Managers

"It takes six or more months to fill a cybersecurity position"



29% of Managers

"Less than a quarter of applicants are qualified for the cybersecurity position"



40% of Managers

"University graduates in cybersecurity are not prepared for the job challenges they will face"

Source: www.isaca.org

Cybersecurity at the national level

The increased **complexity**, pace, scale and interdependence of technological trends will **overwhelm** the current **cybersecurity** postures.

To reap the benefits and manage the challenges of digitalization, countries need to **frame** the proliferation of **ICT-enabled infrastructures** and services within a comprehensive **cybersecurity policing effort**

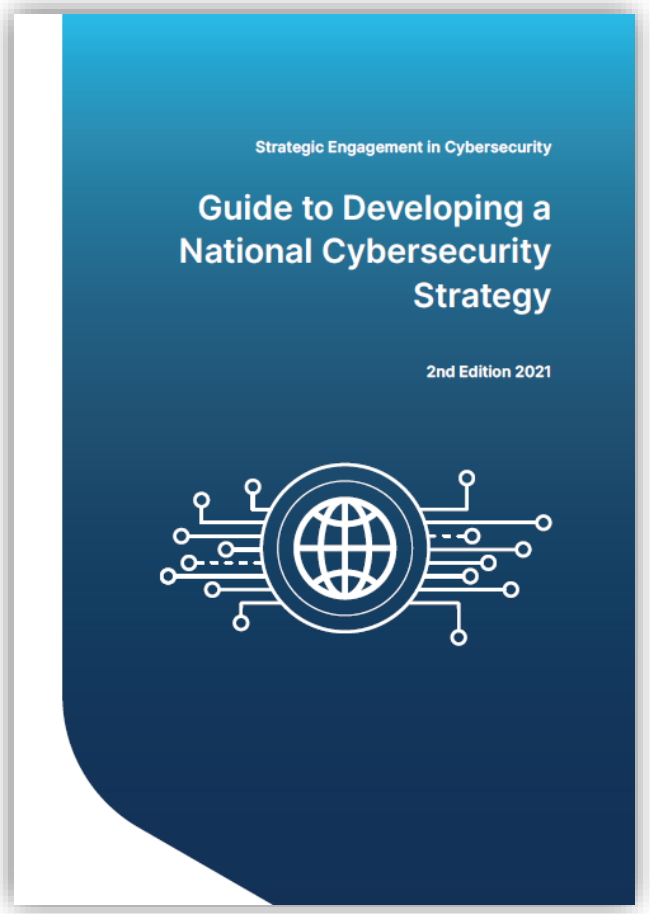
Cybersecurity policy making

governments have a unique and expansive role:

Protect their own infrastructure
Protect national interests:

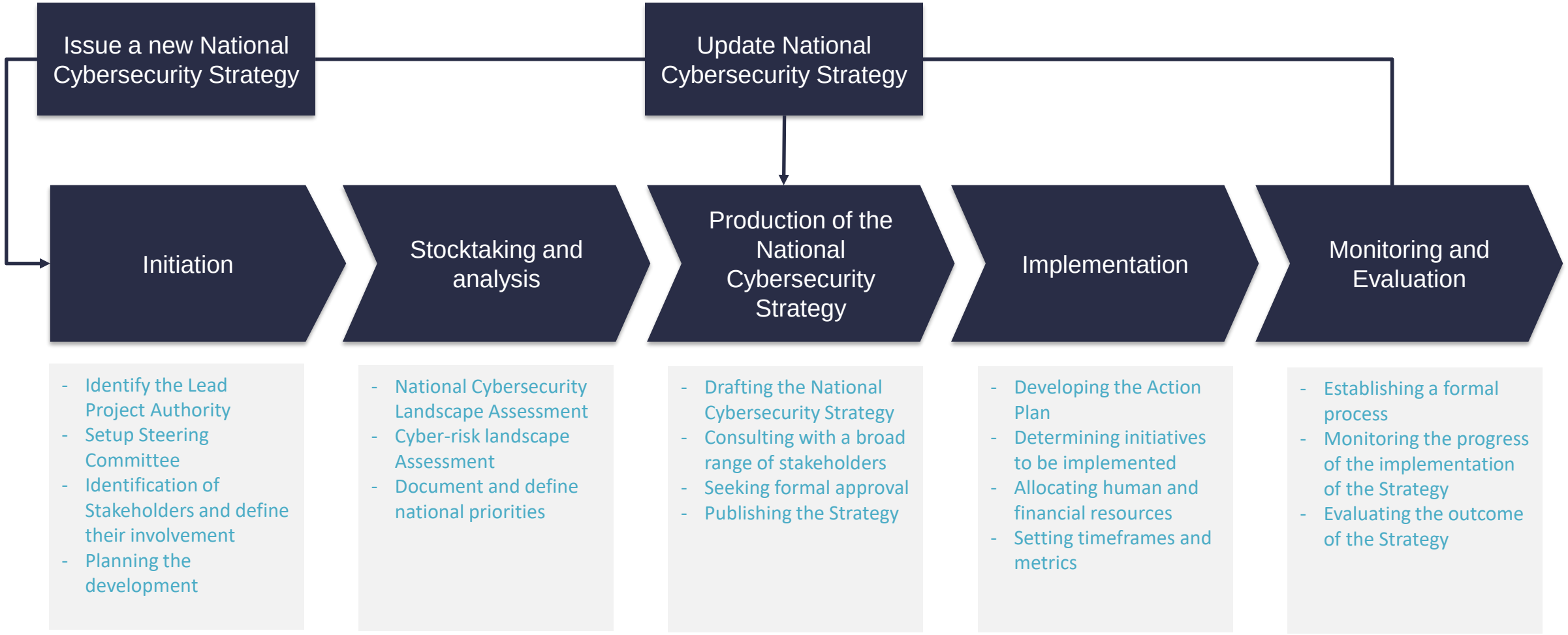
- **Digitalisation**
- **Economy**
- **Human rights and liberties**
- **Citizen and businesses**
- **Build trust environment**

3 Pillars

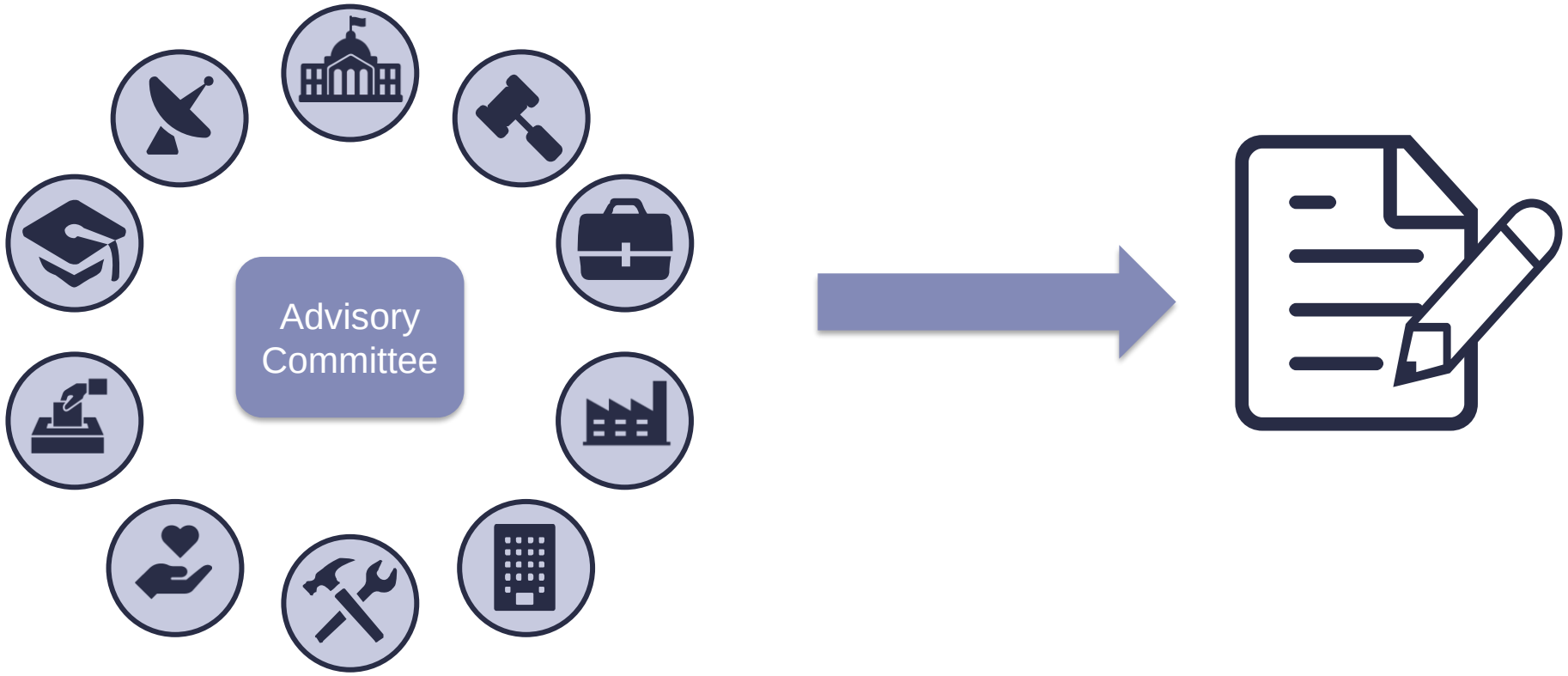


- Lifecycle of a National Cybersecurity Strategy
- Overarching Principles of a National Cybersecurity Strategy
- National Cybersecurity Strategy Good Practices

Cybersecurity and Digital Transformation



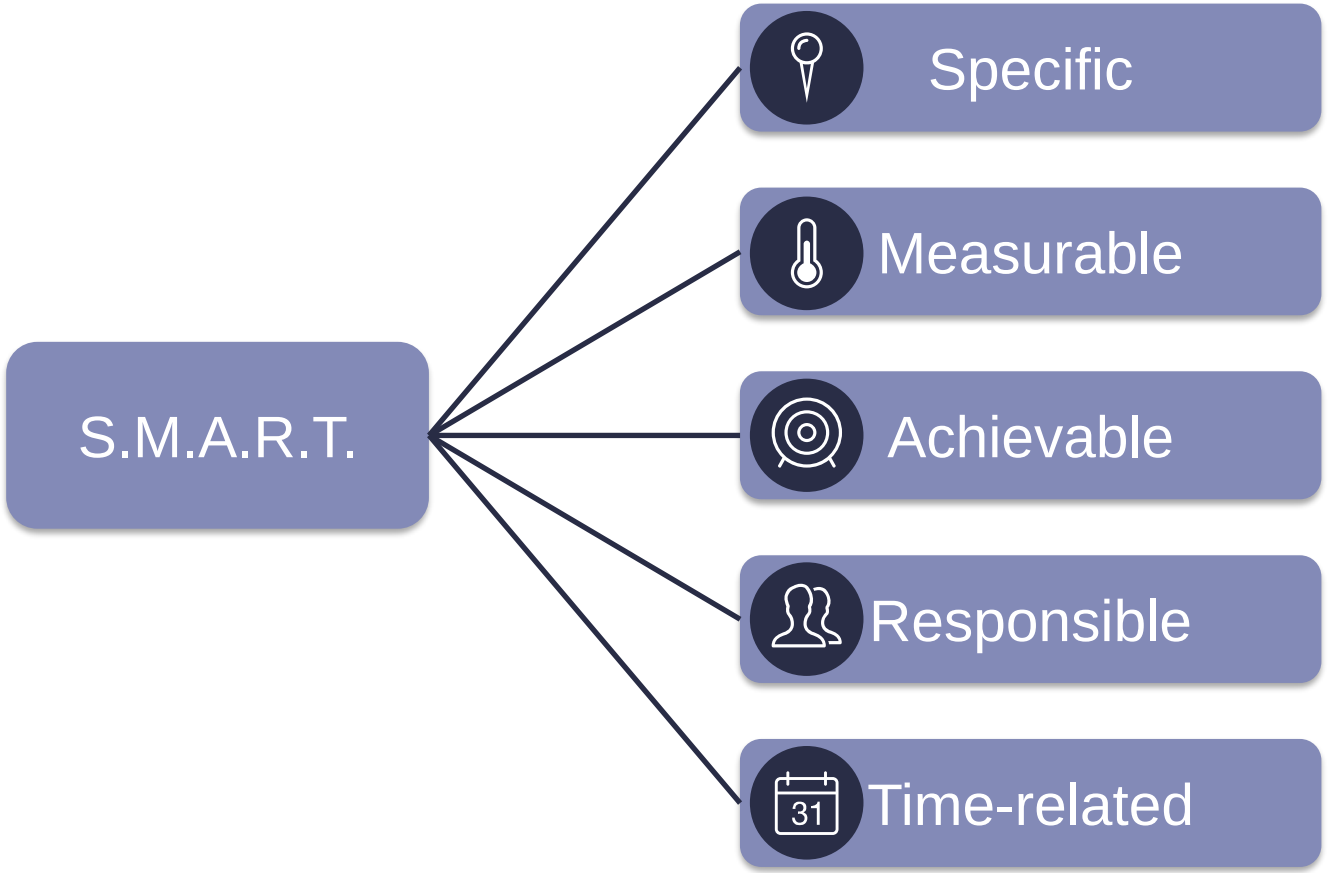
Stakeholders involvement



1. Governance

- Ensure the highest level of support
- Ensure inter-sectoral cooperation
- Establish a competent cybersecurity authority
- Allocate dedicated budget and resources
- Ensure intra-government cooperation
- Develop an implementation plan

Establishing a formal process



THANK YOU

cybersecurity@itu.int
gci@itu.int