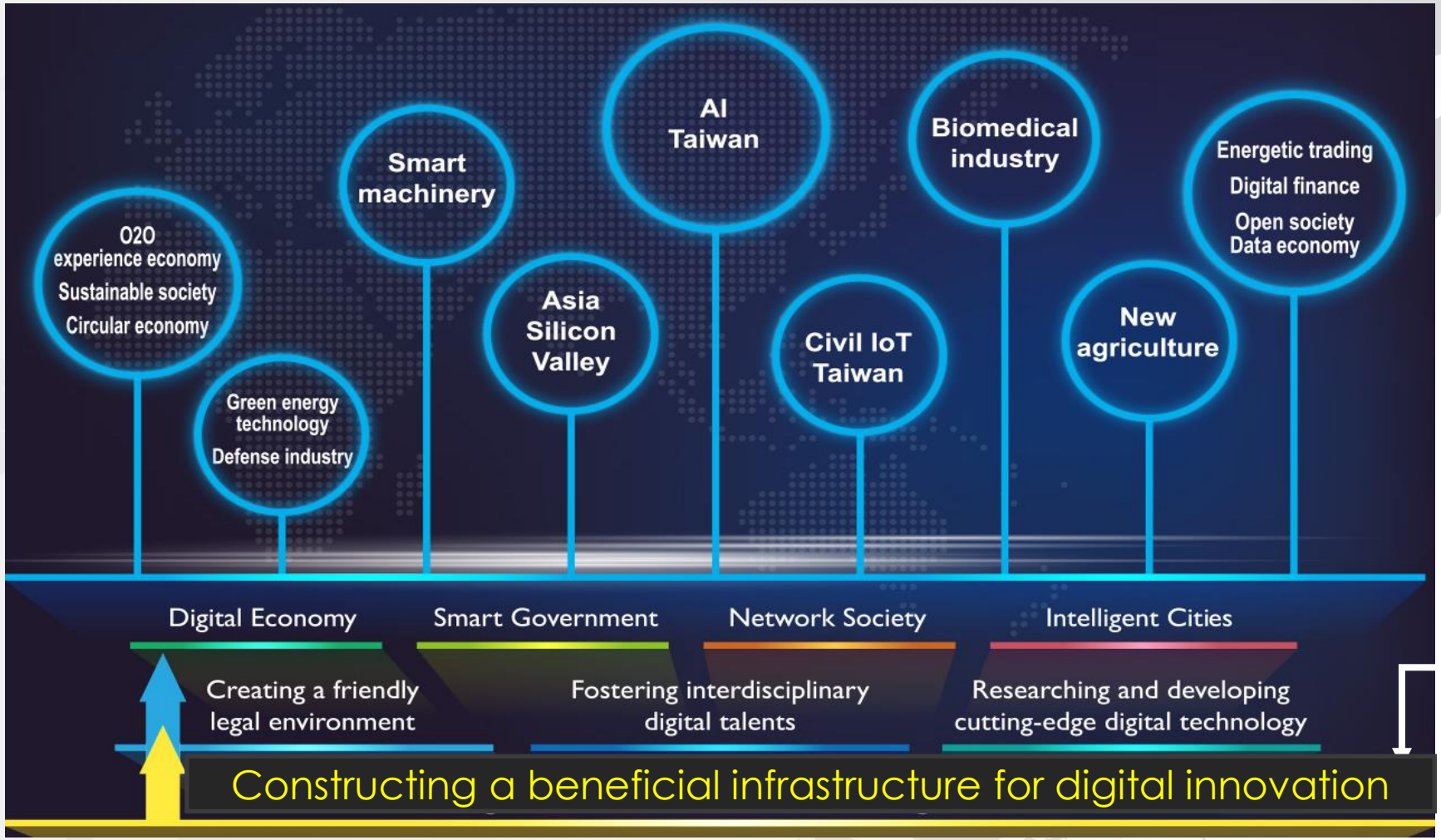
# Digital Technology and Democracy in Taiwan

Dr. Yeali S. Sun, Commissioner

Taiwan National Communications Commission (NCC)

# Taiwan’ s National Policy: “Digital Nation, Smart Island”

- **Digital Nation, Innovative Economic Development Program（DIGI+ 2017-2025)**
- **To accelerate Industrial Innovation and Economic Prosperity**




5+2
Focused
Industry
Sectors

5G

# Highly Developed Broadband Internet Access Services in Taiwan

- PSTN Licenses : 16
- Subscribers: 11,453,595
- **Broadband Subscribers: 4,476,292**

**Fixed Networks**

**Wireless**

- **3G Licenses: 5**
- **4G Licenses: 9**
- **Voice Subscribers : 28,656,487**
- **Broadband Subscribers : 24,427,934**
- **5G Licenses (2020)**

**Size: 36,200 km²**
**Pop: 23.54 M**

- Radio Licenses (AM, FM and SW): 171
- DVB-T Licenses : 6

**Broadcasting**

**Cable**

- **Licenses: 65**
- **Subscribers: 5,225,255**
- **Broadband Subscribers : 1,346,602**

- Satellite Licenses:
  - Fixed: 4
  - Live Broadcasting: 5
- Channel Licenses: 290

**Satellite**

**Internet**

- **IASP Licenses: 225**
- **IXP Providers: 4**

Source: NCC in 2017

# Digital Era: Challenges and Threats in Democratic Taiwan

- We are embracing and maximizing the upside of digital technology at full speed (e.g., expediting digital transformation in all sectors)
- While undertaking progressive digitization of many facets of our society and economy, we are encountering and combatting the cyber threats and various societal and economic issues brought in by the technology such as
  - Disinformation
  - Hacking and theft of online public and private information

➢ **How to mitigate the threats to our open society and national security is an imperative issue!**

# What are our Priorities to **defend democracy?**

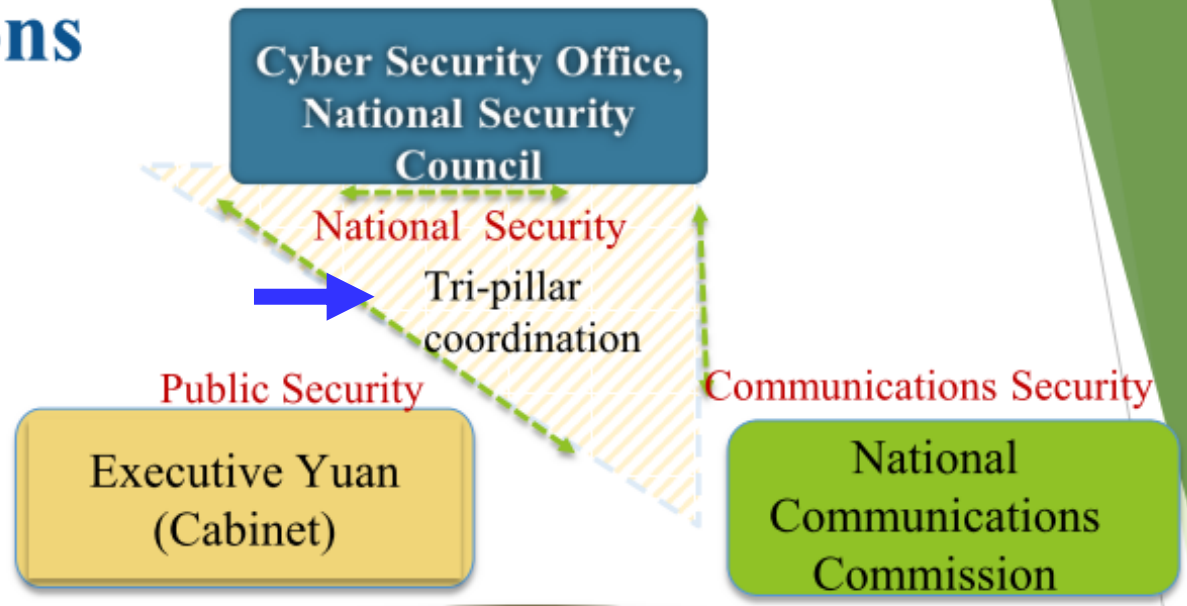
- "Cybersecurity is national security"
- Free and Fair Elections

# Nation-state Cyberattacks

- The attack vector continues to evolve and accelerate.
  - Efforts to acquire and steal technology, classified information and trade secrets of critical industry and high-tech companies
  - Developing a network of scientific, academic and business contacts to collect information and to infiltrate
- The damage has been increasingly borne by the private sector.
  - the *intended victim* or the *unwitting pawn* in an attack on other companies

# Our Missions

Cybersecurity Management Act, (Jan. 1 2018)




**Missions**

- To optimize National Cybersecurity mechanism for assuring homeland security and sustainable digital economy
- To strengthen Protection of Critical Information Infrastructure
- Promote and develop public-private partnerships to enhance mutual trust through collaborations, consolidated defense and information sharing

**EIGHT Critical Infrastructures**

① Energy
② Water
③ **Communications**
④ Transportation
⑤ Banking and Finance
⑥ Emergency Services and Public Healthcare (hospitals)
⑦ Hi-Tech Industrial Parks
⑧ Government

# National communications sector protection: mission and goals

- ✓ Tailor the regulations, strategic guidelines and mechanisms to the unique operating conditions and risk landscape of Taiwan’ s communication sector.

# Communications Sector’ s Security and Resilience Project (2017-2020)


中央災害應變中心 災害情報站 Central Emergency Operation Center.

N-CERT NCCST

N-ISAC NCCST

## National Communications & Cyber Security Center (NCCSC)

**C-NOC**
Collect, integrate and analyze information & events from the six segments

**C-SOC** 1
Identify Threats and Attacks and Situation Awareness

**C-CERT** 2
Event Reporting & Incident Response

**C-ISAC** 3
Information & Threat Intelligence Sharing and Analysis

**Public Sector**

4 Public-Private Partnership

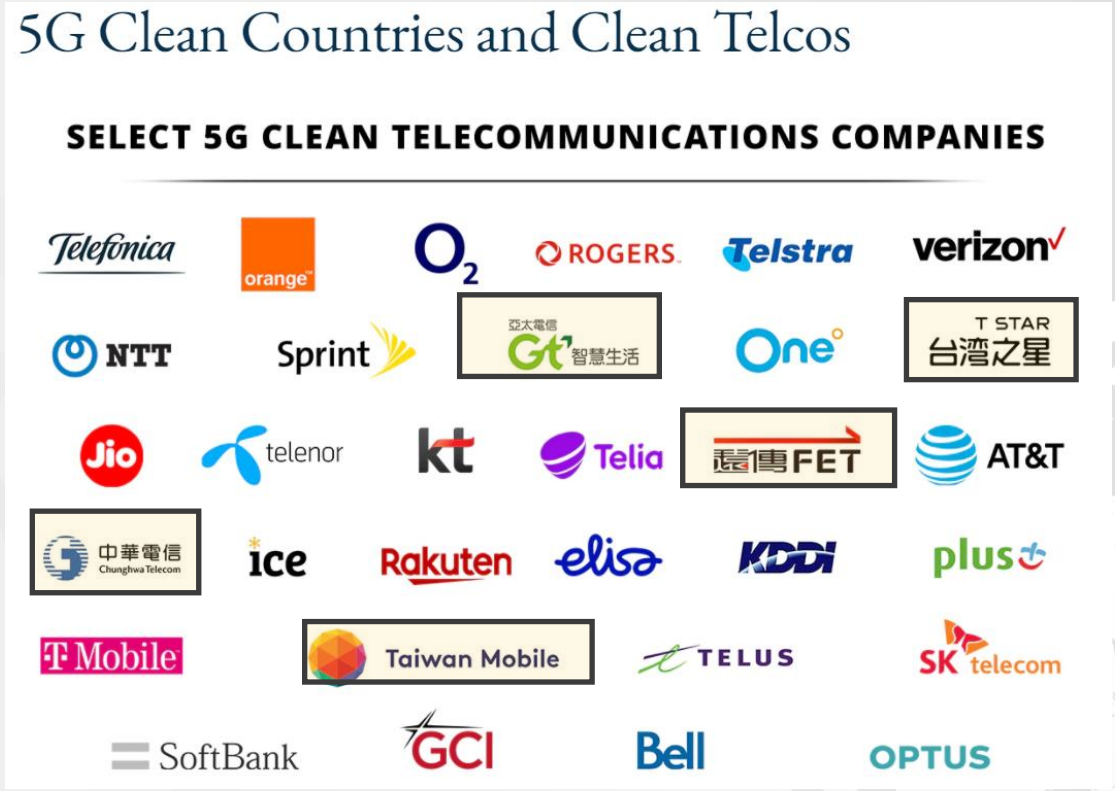
**NOCs**

Cable | Broadcasting | Satellite | Fixed Network | Wireless | Internet (IASP, IXP, DNS)

**Private Sector**

# Secure Communication Sector in Taiwan

- #1 - Ban of Chinese-made equipment in 4G and 5G, and all communications networks.
- #2: Security by design




US-Taiwan
5G Security
Joint Declaration
on August 26,2020

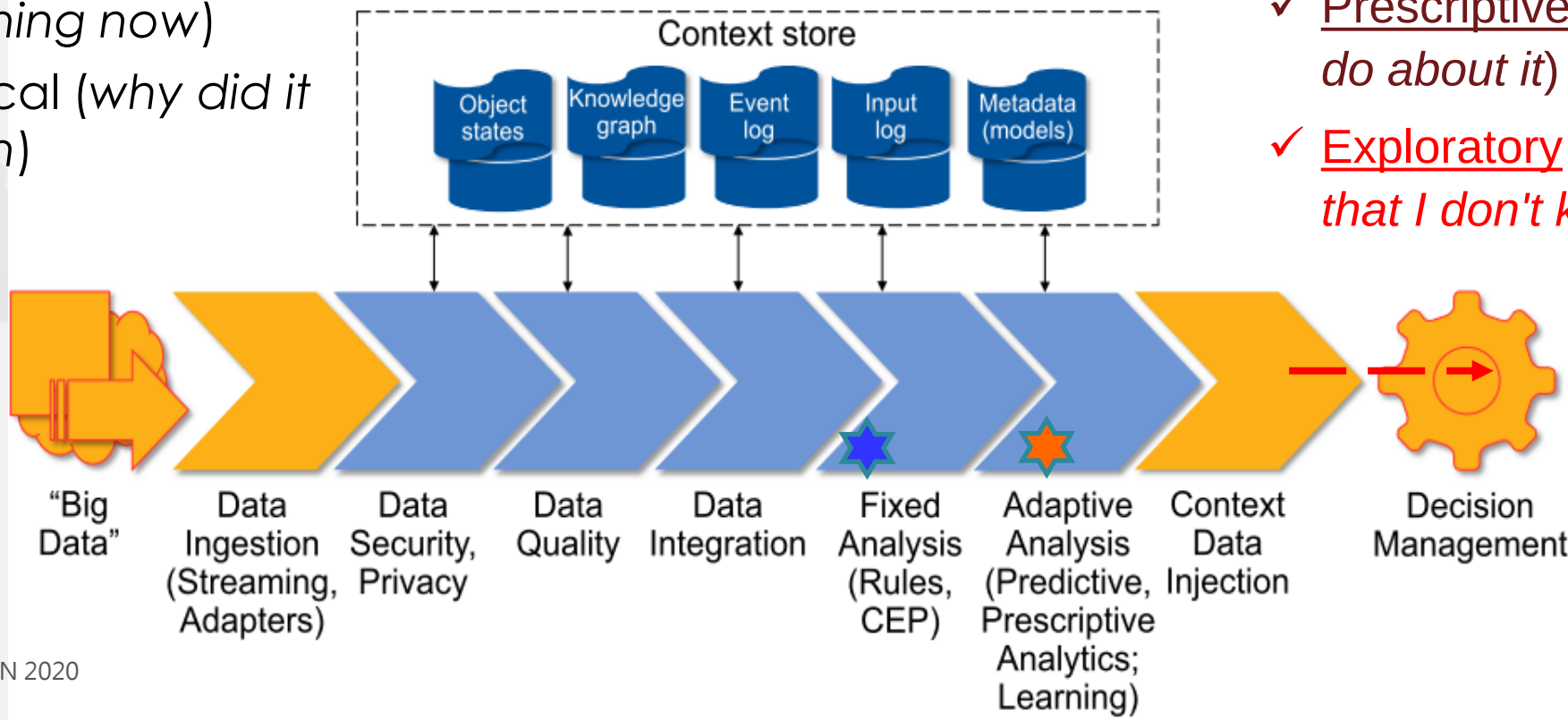
# Defense In-depth at Scale

Q1: Can we gain *better* and *in-depth* understanding and insights of what attacks or attempts are?

Q2: Can such knowledge help us **prevent** cyber attacks, **reduce** cyber risks and better **govern** **the whole cybersecurity process?**

# Proactive Defense In-depth at Scale:
## Analytics Capabilities: Data Analysis, Machine Learning and AI

- Historical (*what has happened*)
- Operational (*what is happening now*)
- Analytical (*why did it happen*)




- ✓ Predictive (*what might happen*) (what-if)
- ✓ Prescriptive (*what should I do about it*)
- ✓ Exploratory (*what's out there that I don't know about*)

Source: Gartner

# Free and Fair Elections

# Disinformation in Taiwan 2018 Elections: threat and challenge

# Channels of Dissemination of Disinformation – Social Media + **Traditional News Media**

- Exerting the impact and influence!

a) **Social media platforms** like Facebook, YouTube, Tweeter, **Line, and PTT** and **24-hour television news stations**.

b) Disinformation or fake news were repeatedly broadcasted, and appeared on users' newsfeed.

c) The "then social media algorithms" tended to generate a *distorted* system in evaluating information (more-reiteration and share of the same info -> more popular).

d) Every social media user can be a news publisher.

e) The use of troll and bots on social media (i.e., fake accounts ) to *trend* the disinformation, and make them visible, i.e., reaching out.

# Disinformation Threat in 2018 Elections


- The threats brought in
  - Created **tensions** between populace and within society and nation
  - **Polarized** and **fragmented** the society
  - **Undermined the trust in government** and political leaders
  - **Destablized** society and state
  - **Manipulated psyches of the population** (casting doubt and public cynicism)

➢ Big Threat to Democracy

➢ Delegitimizing the power and authority of the government

# Government Emergence Response Team to Disinformation (1/2)

## Step 1 – Clarification

### Q1: Who is in charge?

A1:

- Government agencies, third-party fact-checking institutes, media literacy …
- Principles
  1) **To be effective, rapid response and timeliness**
  2) Reachableness of incident response, comparable with the rapid speed and coverage of the dissemination of disinformation?
- Almost every agency created an official account on MAJOR social media platforms such as FB and line to post clarification messages.

# Government Emergence Response Team to Disinformation (2/2)

## Step 2 – Attribution

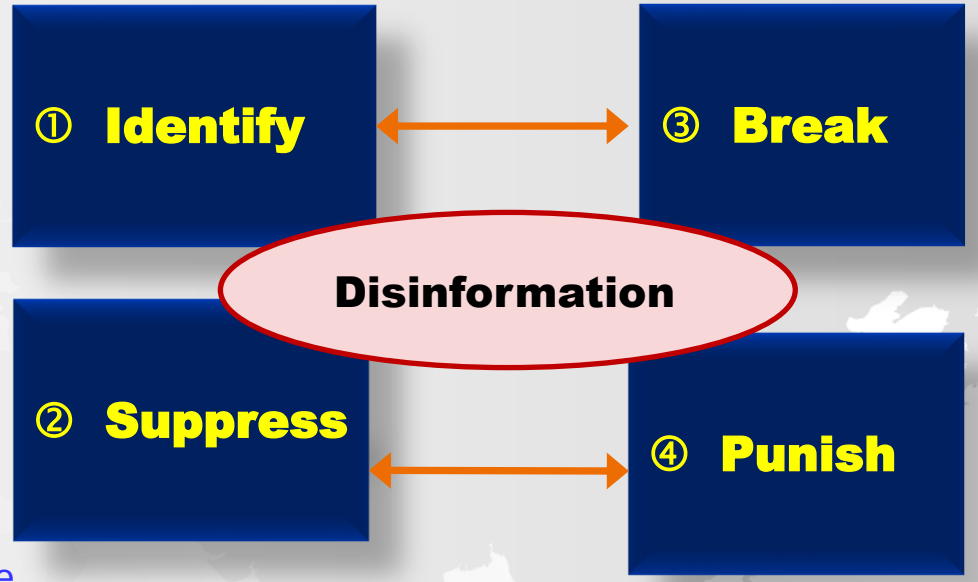
Q2: How to find the disinformation sources, actors and perpetrators accountable?

A2: Very difficult …

- Nation-state disinformation-specific cyber attacks have been continuing to evolve and accelerate.

# FOUR Strategies to Combat Disinformation while Protecting Freedom of Speech

- Prevention
  - Media Self-regulation
  - Enhance media literacy, and develop independent judgment
  - ➢ Transparency
  - ➢ Openness
  - ➢ Trust
- Suppression
  - Strengthen cooperation between Gov. and Media
  - Effectively curb the spread of harm (Both legal and technology)
  - Supervision by the Public




- Improve the efficiency of the clarification mechanism
- Leverage third-parties' help and momentum on fact-checking
- ➢ Rapid response and Timeliness
- Impose illegal liability
- Harden legal system
- Ensure fair and independent judicial review
- ➢ security and human rights

- At Cabinet-level and Ministry-level every gov. agency establishes a fact-clarification area

# NCC Media Regulations: Fact Checking and Verification

- **Fact checking principles in the Satellite Broadcasting Act (2016)**

  "… prevent instances such as misinformation, false context, sensationalism, exaggeration, and media bias …"

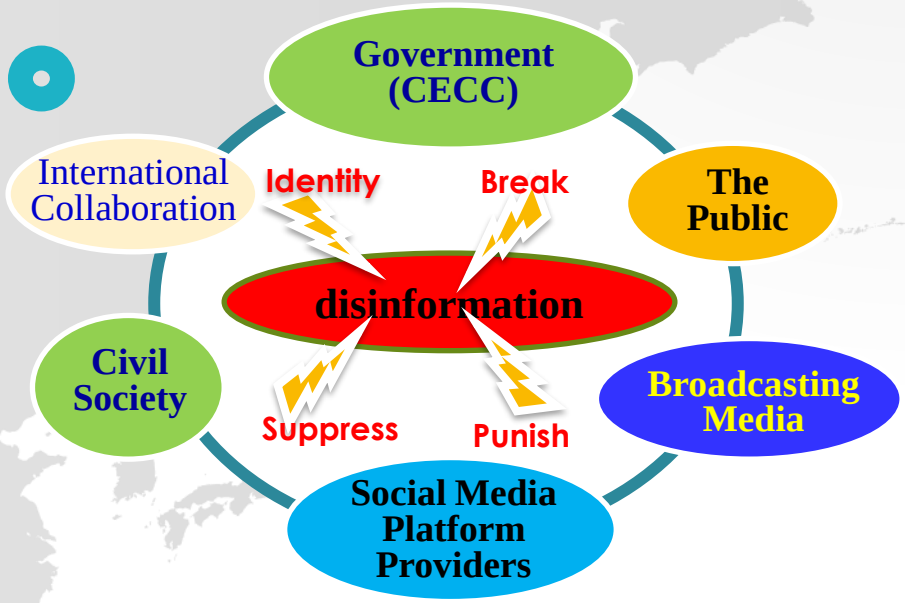
  - **Media outlets have responsibility to provide reasonable grounds on accuracy** (although it is not required to prove authenticity of the evidence and sources of information presented)

- NCC established a **fact verification guideline** in 2018 for broadcasting industry to follow.

# ALL Major Stakeholders Must Collaborate

1) **Taiwan government responds rapidly** and takes **appropriate actions** in combatting disinformation
2) **Strict legal system**
3) **Use of Technology**
4) **Involving all major parties** including government agencies, ISPs, social media platform providers and civil societies
   - All are actively collaborating and cooperating with each other on information clarification and stopping dissemination of disinformation.
5) **Taiwan people strictly comply with the orders** from CECC and the law
6) **Taiwan people are more literate and smart** in terms of recognizing false information and not forwarding doubtful information

→ Strong partnership and cooperation between the government and private sector

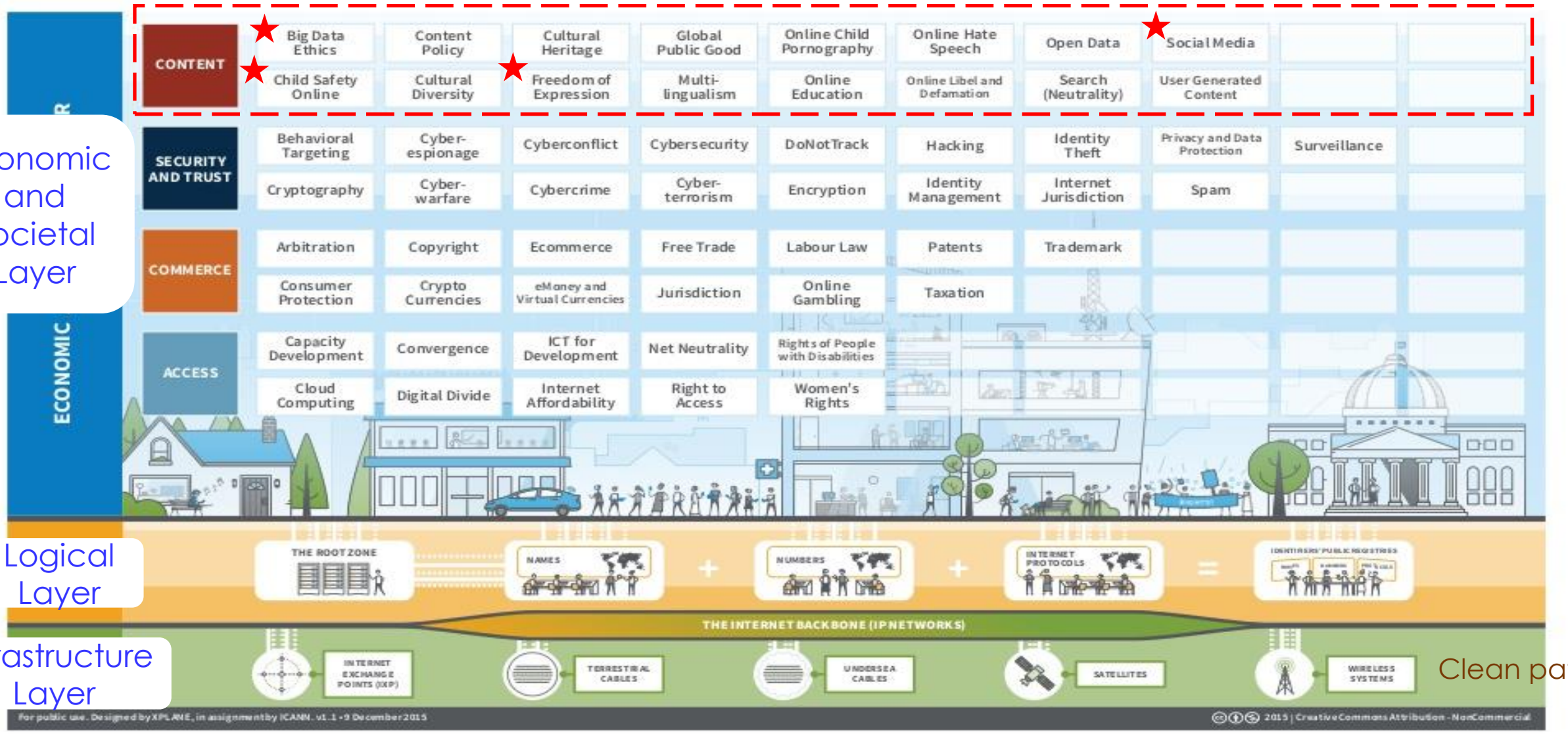


# Concluding Remarks

- **Digital nation and promoting innovative economic development are our national policies.**
  - expediting digital transformation in all sectors
- Cybersecurity is national security"
- The privacy protection and security battle in digital age is just on …
- **Cybersecurity capability building** is imperative for network operators, service providers **and** regulatory government agency.

# Digital Governance

**Content: big data ethics, child safety online, freedom of expression, social media**




Economic and Societal Layer

Logical Layer

Infrastructure Layer

Clean path

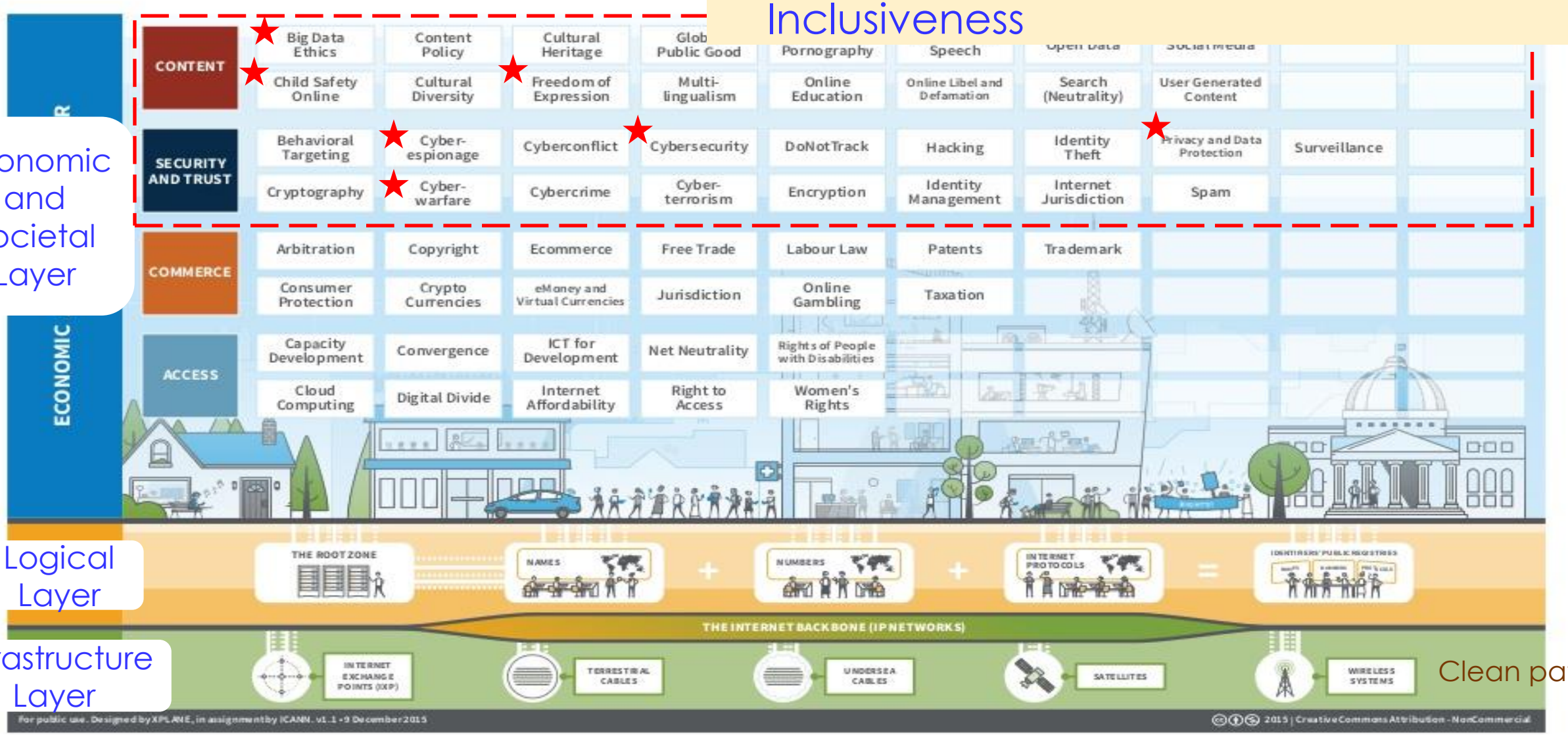


Source: ICANN (Internet Corporation for Assigned Names and Numbers)

# Digital Governance

## Network Governance: Principles

- Multilateralism, Transparency, Democracy, Multistakeholderism and Inclusiveness






Source: ICANN (Internet Corporation for Assigned Names and Numbers)

Thank you. ☺