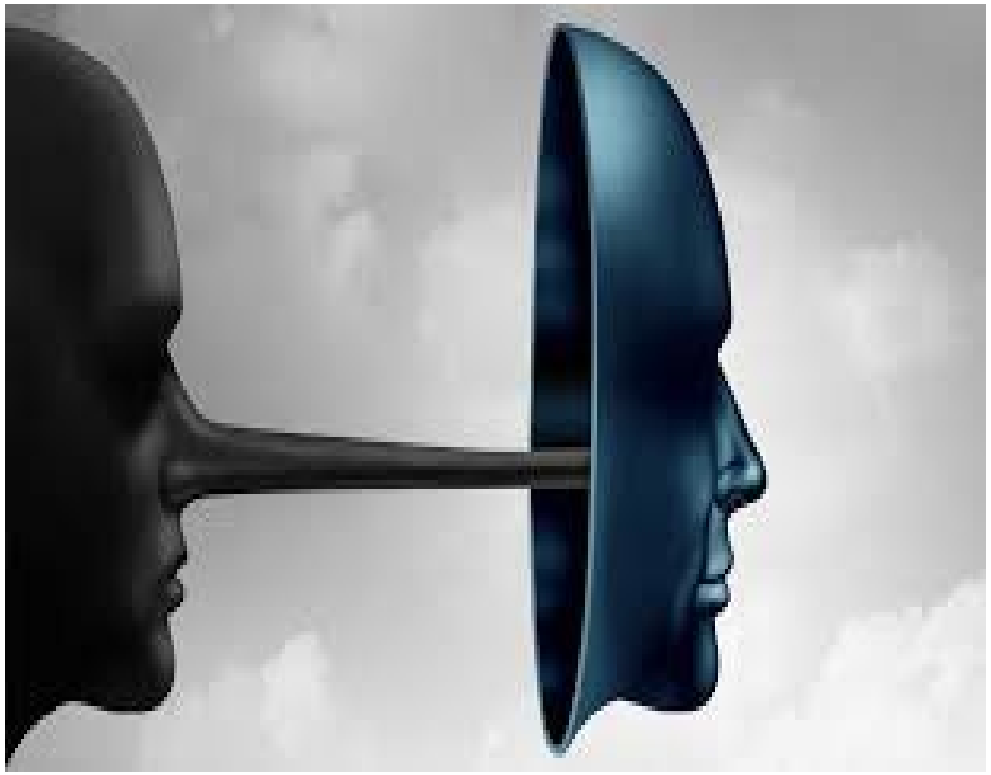
FAKES
A Global Phenomenon



Lily Ong
Geopolitics360

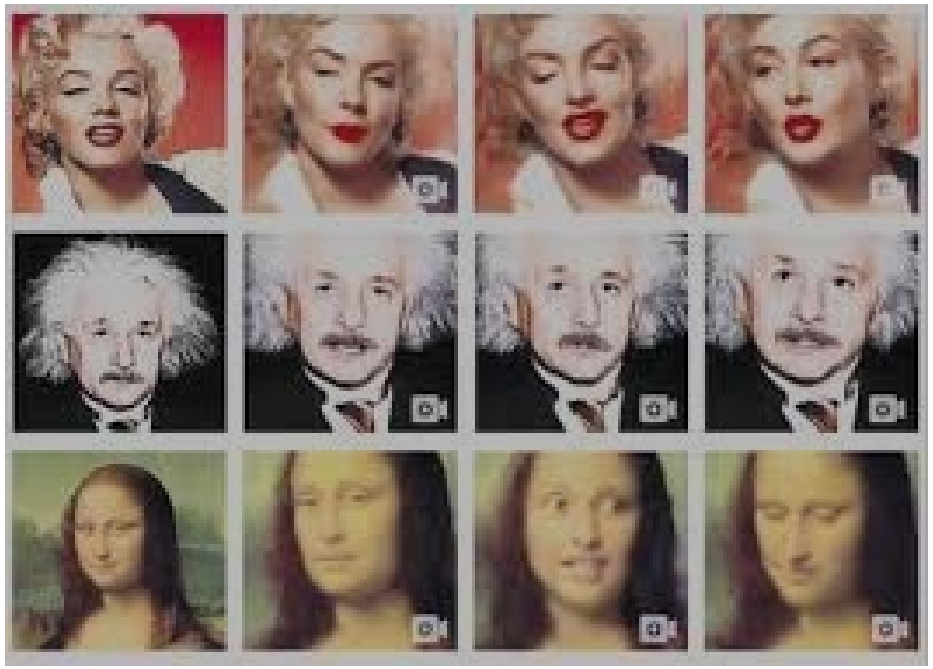
Global Phenonemon of Fakes

Universal rise in:

- Number of fakes
- Technological advancemen
- State involvement
- Response strategies
- Regulatory efforts

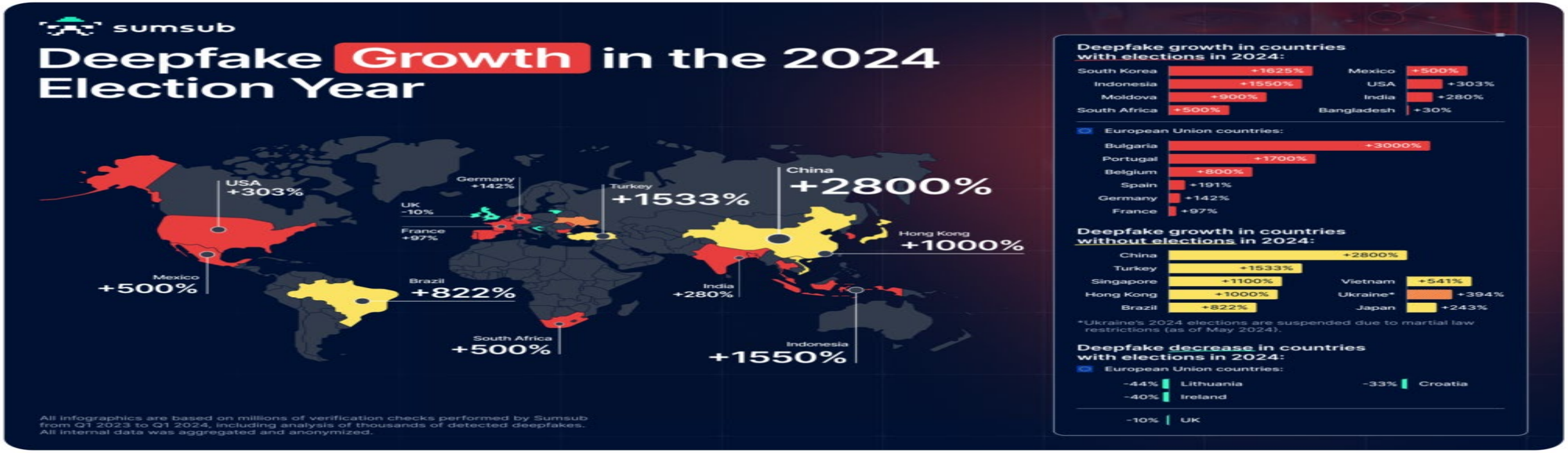
International I

- Deepfakes to reach 8 million by 2025; 16 times > 2023 (500,000)
- 2024: +118% in deepfakes and AI audio
- Deepfakes 7% of global fraud; overall scams +4 times
- APAC Deepfakes: Singapore and Cambodia (+240%); SK (+735%)



Internation
al II

- Worldwide financial sector (+2137% over three years)
- #1 ATO; #2 payment card; #3 phishing
- AI 42.5% of financial fraud (compared to 0.1% in 2021)
- Deepfakes 1 in 15 incidents
- Teenagers: deepfakes nudes (12%)

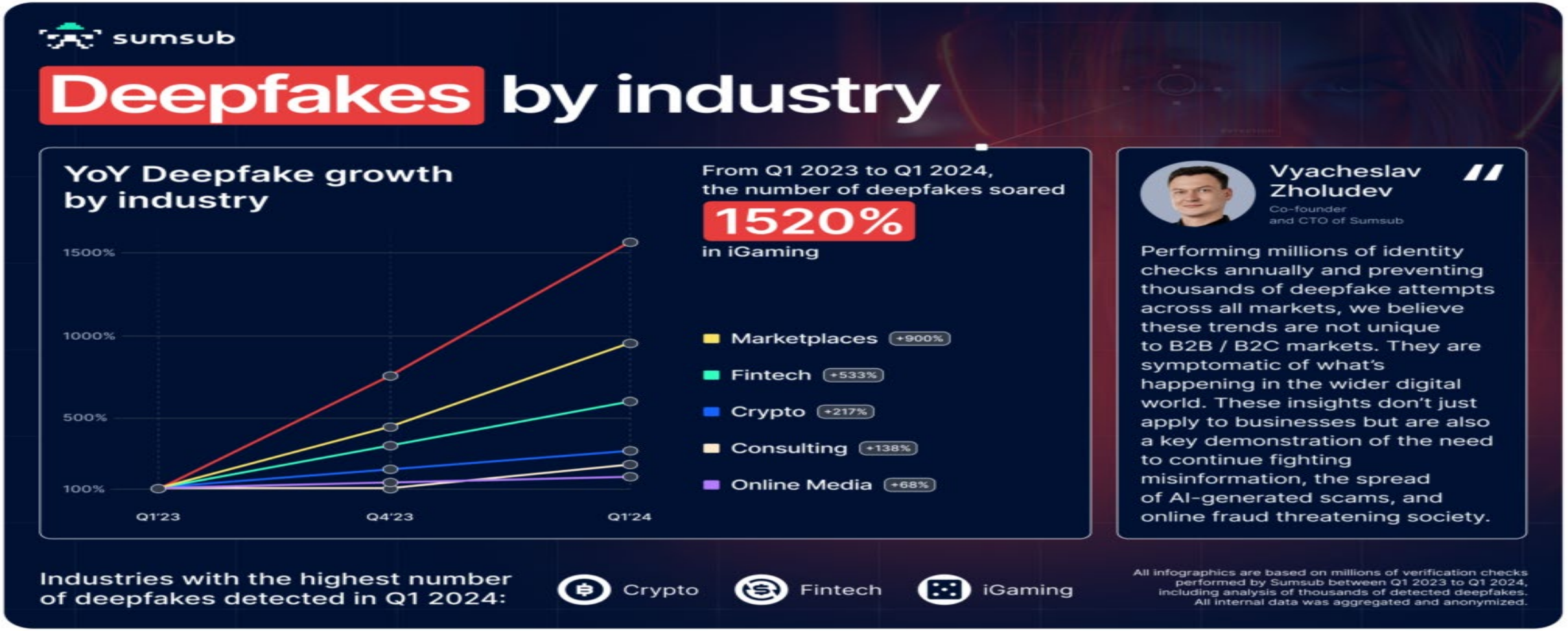


Most deepfakes Q1 2024: China, Spain, Germany, Ukraine, US, Vietnam, UK

Elections 2024: India (280%), the US (303%), South Africa (500%), Mexico (500%), Moldova (900%), Indonesia (1550%), and South Korea (1625%).

EU: (European Parliament elections): Bulgaria (3000%), Portugal (1700%), Belgium (800%), Spain (191%), Germany (142%), and France (97%).

Huge Rise: China (2800%), Turkey (1533%), Singapore (1100%), Hong Kong (1000%), Brazil (822%), Vietnam (541%), Ukraine (394%)** and Japan (243%).



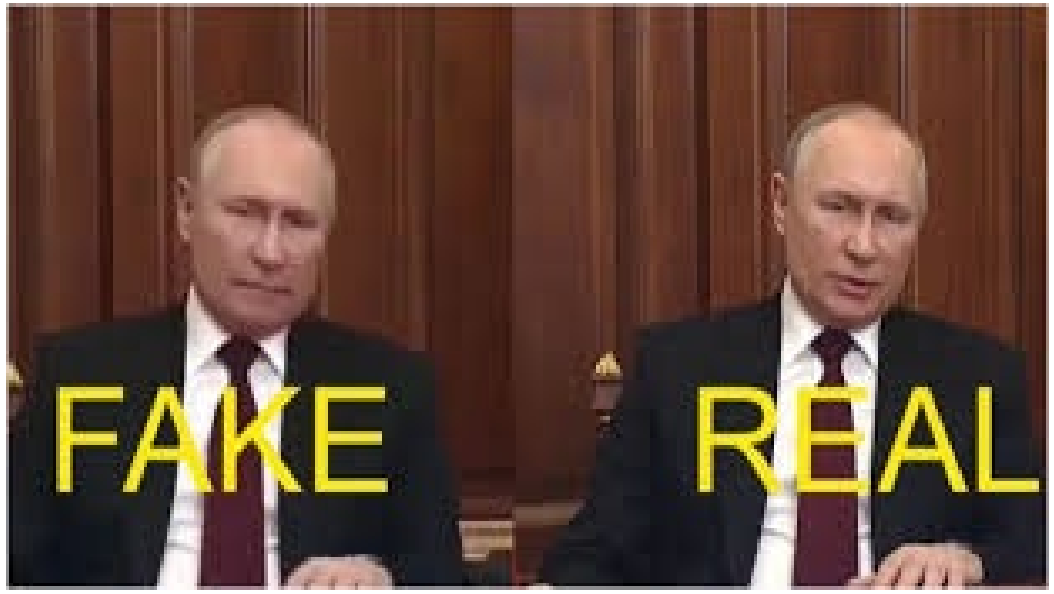
Q1 2024: **crypto, fintech and iGaming**

1520% in iGaming, **900%** in marketplaces, **533%** in fintech, **217%** in crypto, **138%** in consulting, and **68%** in online media.

Russia

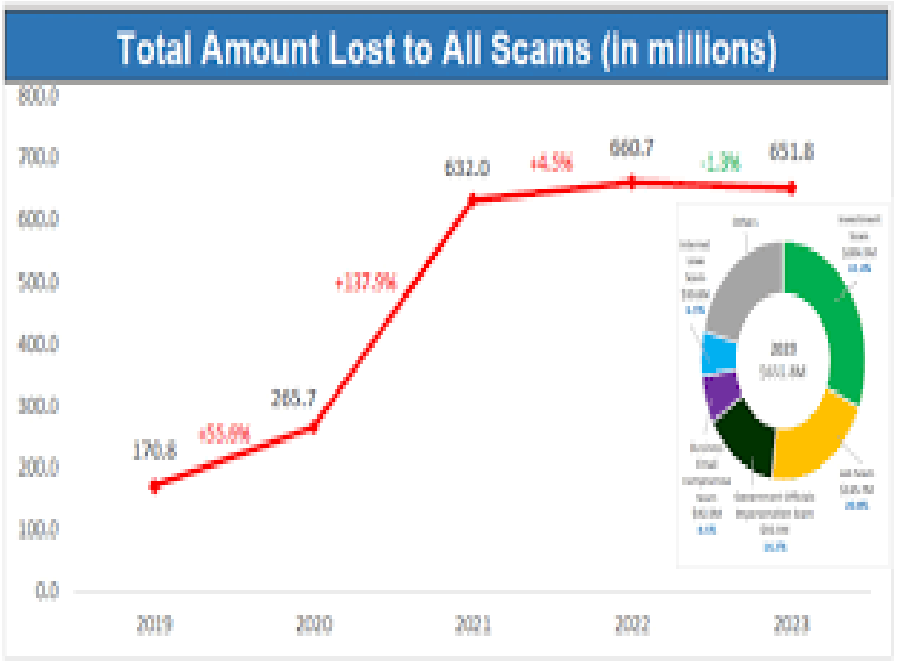
- **2025 Quarter 1**
- 61 unique deepfakes, 2300 copies
- Target: political sphere, govt, state security, regional governors most impersonated
- Deepfakes: 67% of total scams reported, 2.6 times higher than ALL of 2023

- **2024**
- 84 unique deepfakes, 9300 copies
- 3.7 times > 2023
- 45% Odnoklassniki: 20% VKontakte; 18% Telegram; 9% traditional outlets



Scams in Singapore

- 2024 SGD 1.1 billion (70 billion rub); 70% > 2023)
- 25% cryptocurrency
- #1 e-commerce; #2 job; $3 phishing
- 70% under 50yo (e-commerce); elderly (phishing)
- 58% cybercrime victims
- Social media, messaging and online shopping
- OCHA, Sim cards, POFMA, election
- Example: Extortion of politicians



Directive: Remove content or display “true” statement

Penalties: 6 million rubles for

How to Counter Digital Disinformation?

Balancing Security and Free Speech

1. Education

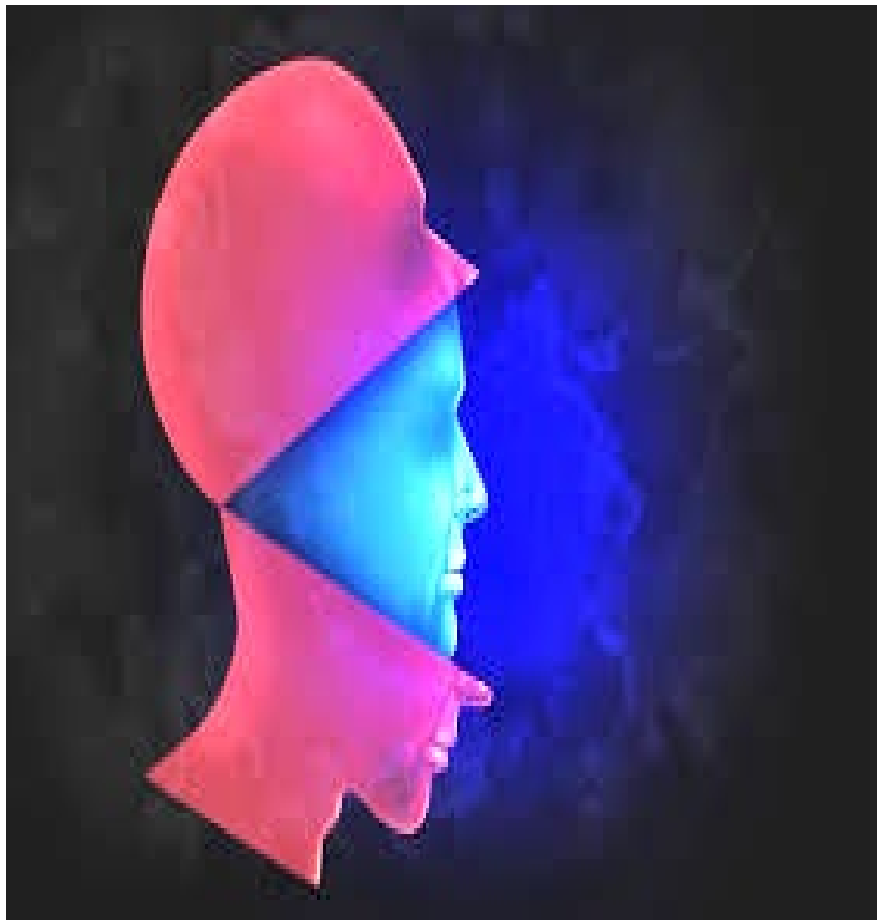
- Media literacy skills
- Parents, caregivers and school, training
- Community workshops, online resources and courses
- Access impact and adapt strategies

2. Collaboration

- Gov’t, tech companies, experts, journalists, psychologists, etc.
- Advisory committees, research partnerships, conferences, networks
- Ethical standards, recognize fact-checkers, showcase
-

Dialogue on Fakes 2.0 Forum Presented Concept of International Fact-Checking Association

3. Utilize Technology



- AI and machine learning to identify disinformation
- Browser extensions
- Promote verified contents
- Source attribution tools
- Data analytics to inform strategies**

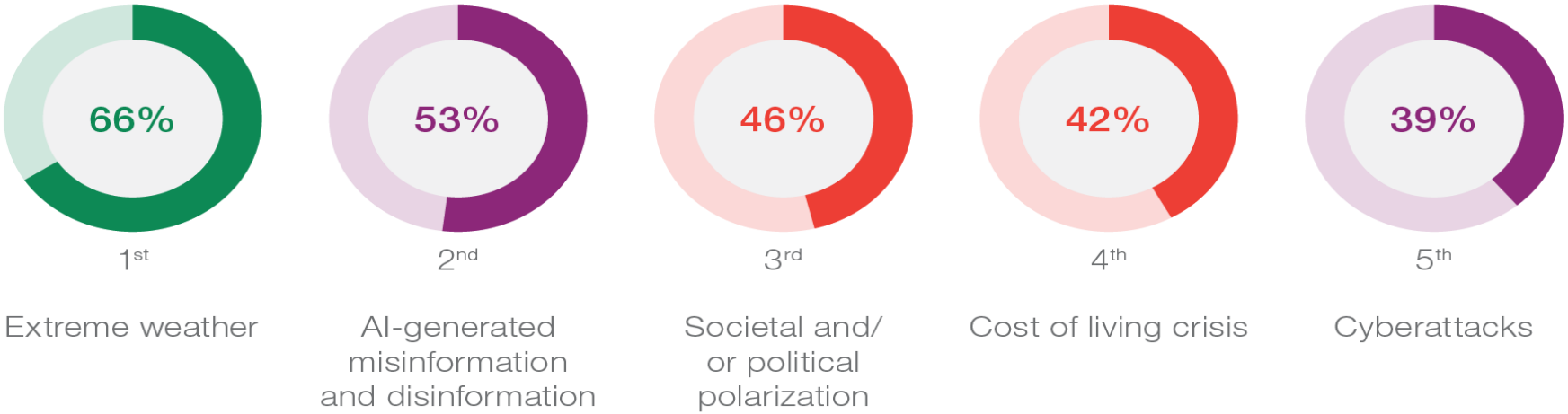
**Beware of privacy intrusion

4. Legislative Frameworks

- Clear definitions
- Disclosure of sources, algorithms, funding, and partners
- Liability standards and reporting mechanism (e.g. complaints)
- Regulate political advertising
- Laws agai edia (e.g. labeling)

5. International Cooperation

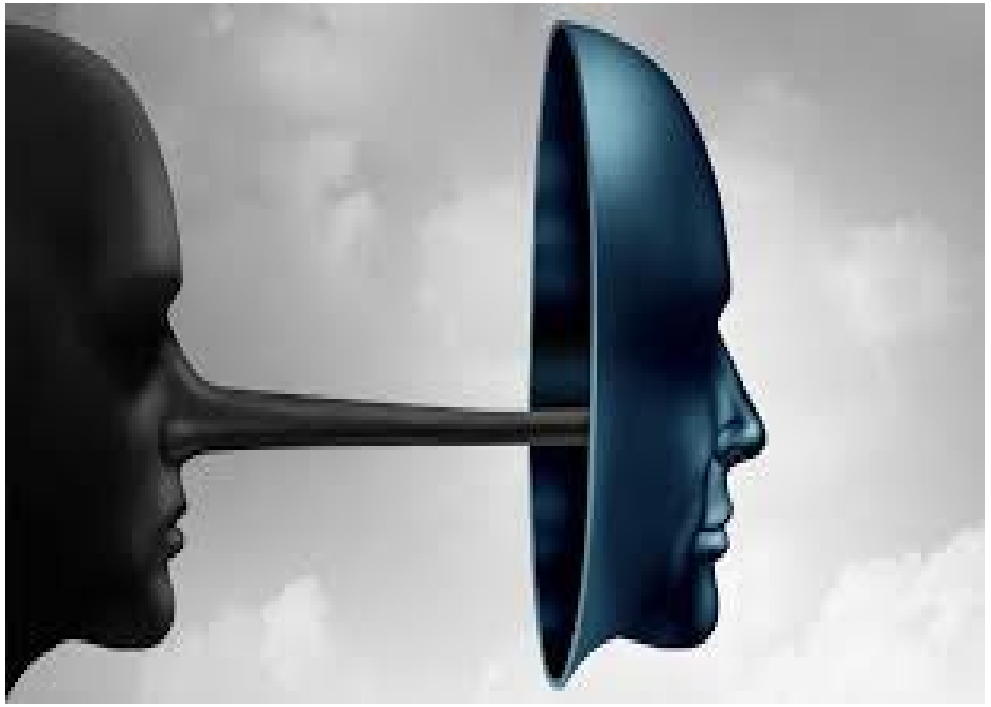
- Global dialogues on cooperation
- Multilateral agreements to address cross-border disinformation
- Establish oversight bodies and committees
- Involve civil society organ



Differences in East-West Approach

1. Regulatory Frameworks
2. Role of Government vs. Civil Society
3. Media Landscape
4. Public Engagement and Media Literacy
5. Cultural Contexts

FAKES
A Global Phenomenon



Lily Ong
Geopolitics360