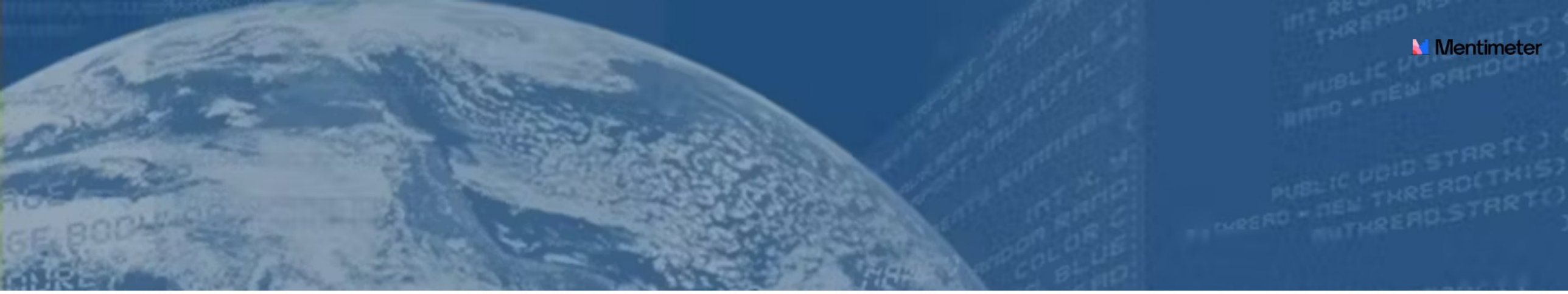
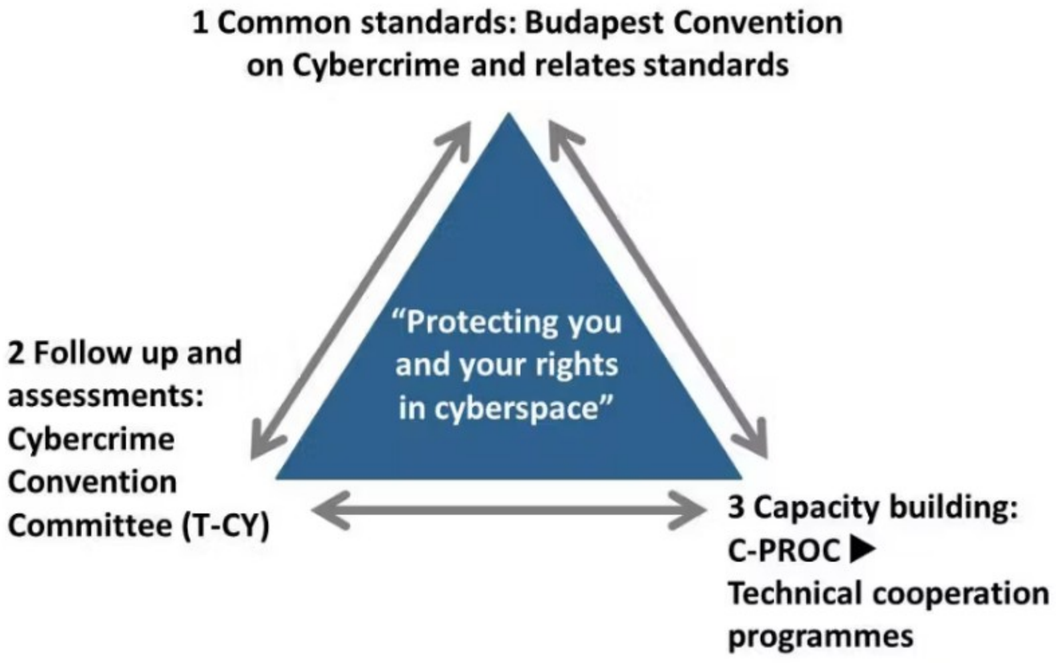


Public-private partnerships in support of action on cybercrime and electronic evidence

Cybercrime Division of the Council of Europe

www.coe.int/cybercrime



Triangle of cybercrime action

- Budapest Convention on Cybercrime and related standards as source of action
- Cybercrime Convention Committee (T-CY) as guardian and enforcer of standards
- Cybercrime capacity building through C-PROC as **tools to support** the states to adhere to these standards

Mentimeter

Capacity building on cybercrime and electronic evidence

- Cybercrime Programme Office of the Council of Europe in Bucharest, Romania:
- 45 staff, 7 projects, funding up to 35 mln EUR
- Close to 400 events per year
- National, global and regional coverage
- Uniform approach to capacity building

Mentimeter

How do we understand public/private partnerships?

- The context of the Council of Europe
- The key question of access to data
- Procedural powers with safeguards
- International cooperation

Mentimeter

Public-private cooperation in the context of capacity building

- Capacity building as source for PPPs
- National standards complementing legislation
- Private partners as direct contributors to capacities of authorities
- Private partners as recipients of assistance

Mentimeter

Capacity building as source for partnerships

- **2008 Guidelines for public-private cooperation:**
- Trust and culture of cooperation
- Quality of requests and procedures
- Knowledge and skills shared on both sides
- ...
- Research and advice: liabilities, strategies, data proteciton, etc.

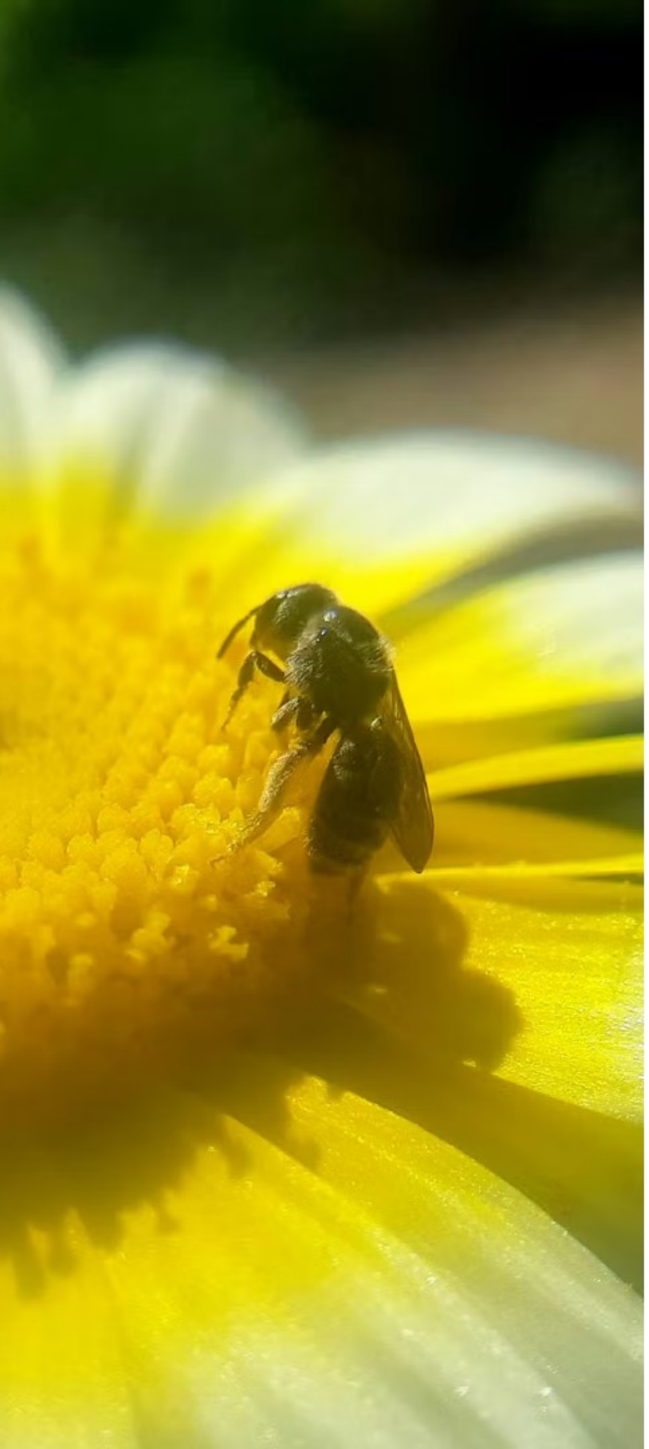
National standards complementing legislation

- Procedural powers with safeguards
- Data retention regulations
- **Cooperation memoranda:**
- Points of contact
- Quality of requests
- Training and skills

Mentimeter

Contribution to capacity building

- Cyber Barometer studies
- Sustaining dialogue in regional and national contexts
- Direct training of law enforcement and prosecutors
- Taking part in cyber exercises
- Advising on implementing the Second Protocol
- Sharing tips and intelligence



Mentimeter

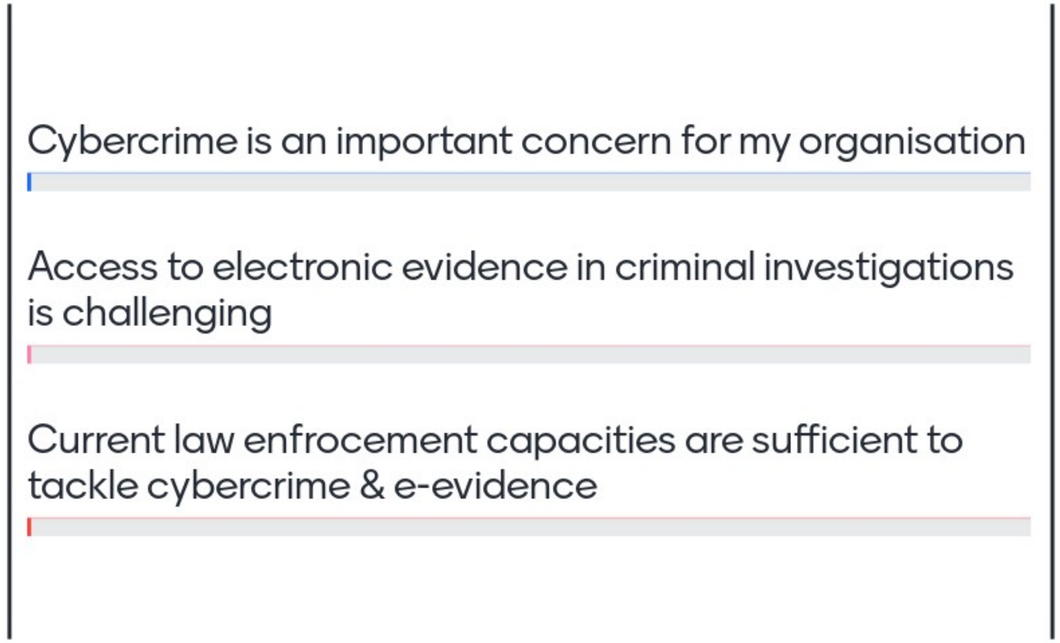
Capacity building for private partners

- Joint cyber exercises
- Procedural powers and safeguards
- International cooperation tools
- Synergies between law enforcement and cybersecurity community
- Networking and contacts

Time to get your feedback!

- Use any device
- Go to menti.com
- Use code 2194 3472
- Responses are anonymous and not tracked
- More than one response welcome

Problem of cybercrime and electronic evidence



Please rank these in terms of importance for current level of public-private cooperation:

1st Clear legislation

2nd Trust /culture of cooperation

3rd Quality of requests

4th Skills and knowledge

5th Contact points

How would you assess the current level of cooperation of your organisation with the law enforcement (not just on cybercrime/evidence)?

What are the current obstacles for public-private cooperation?

What can your organisation offer to the law enforcement in terms of supporting action against cybercrime and electronic evidence of crimes?

What would be the benefits for you from public-private partnership on cybercrime and e-evidence?

Thank you for your attention!