Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

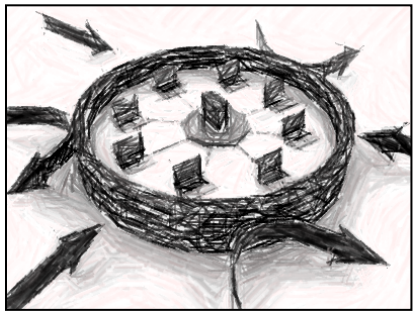
COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Council of Europe action on cybercrime and electronic evidence

Ensuring cyber resilience through cooperation and capacity building



Prepared by the Cybercrime Programme Office of the Council of Europe (C-PROC)

Council of Europe action on cybercrime

1 Common standards: Budapest Convention on Cybercrime and related standards

2 Follow up and assessments: Cybercrime Convention Committee (T-CY)

3 Capacity building: C-PROC Technical cooperation programmes

Scope of the Budapest Convention: Primarily criminal justice response to threats

Criminalising conduct

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools

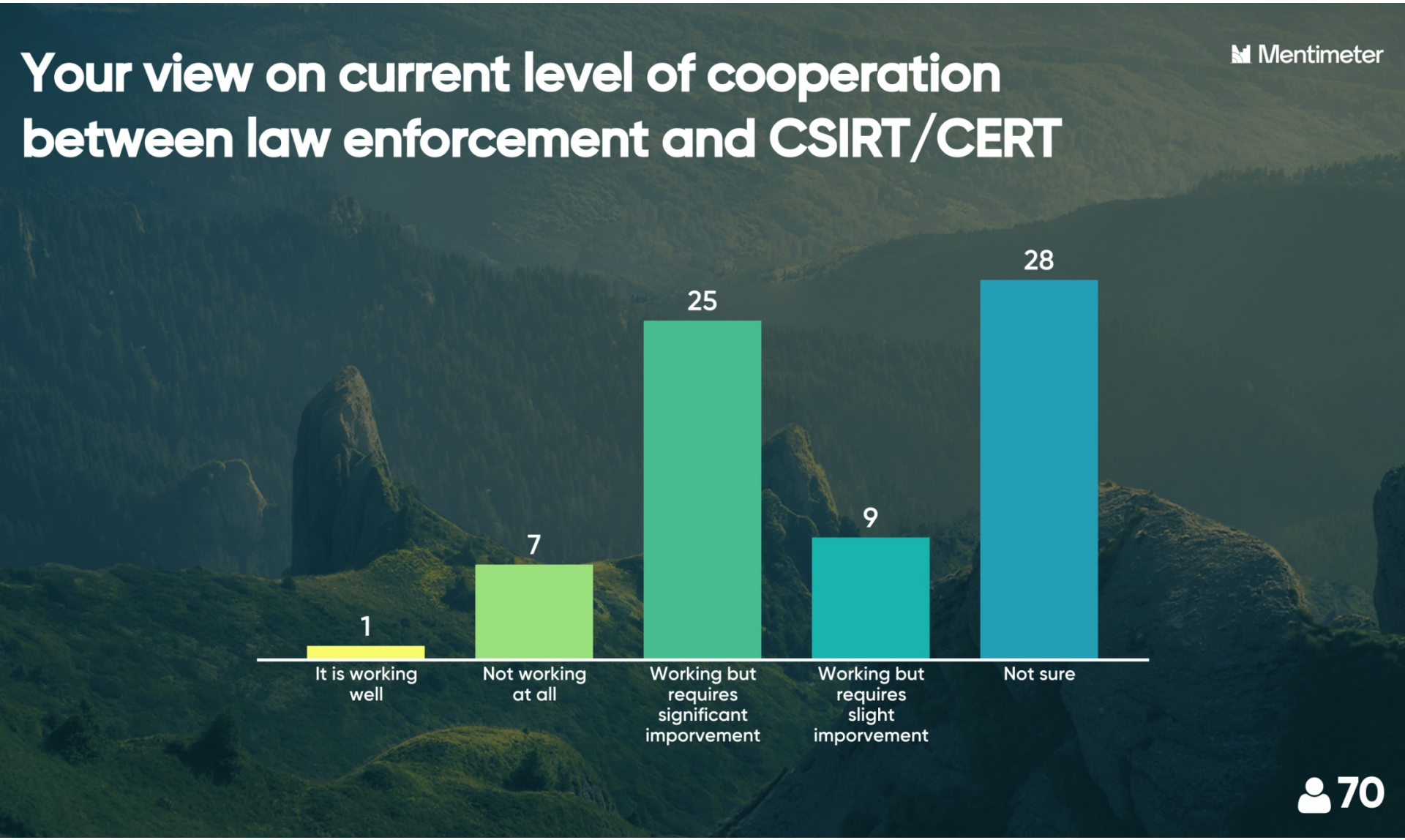
- Expedited preservation
- Search/seizure
- Production orders
- Monitoring/interception of computer data

+

International cooperation

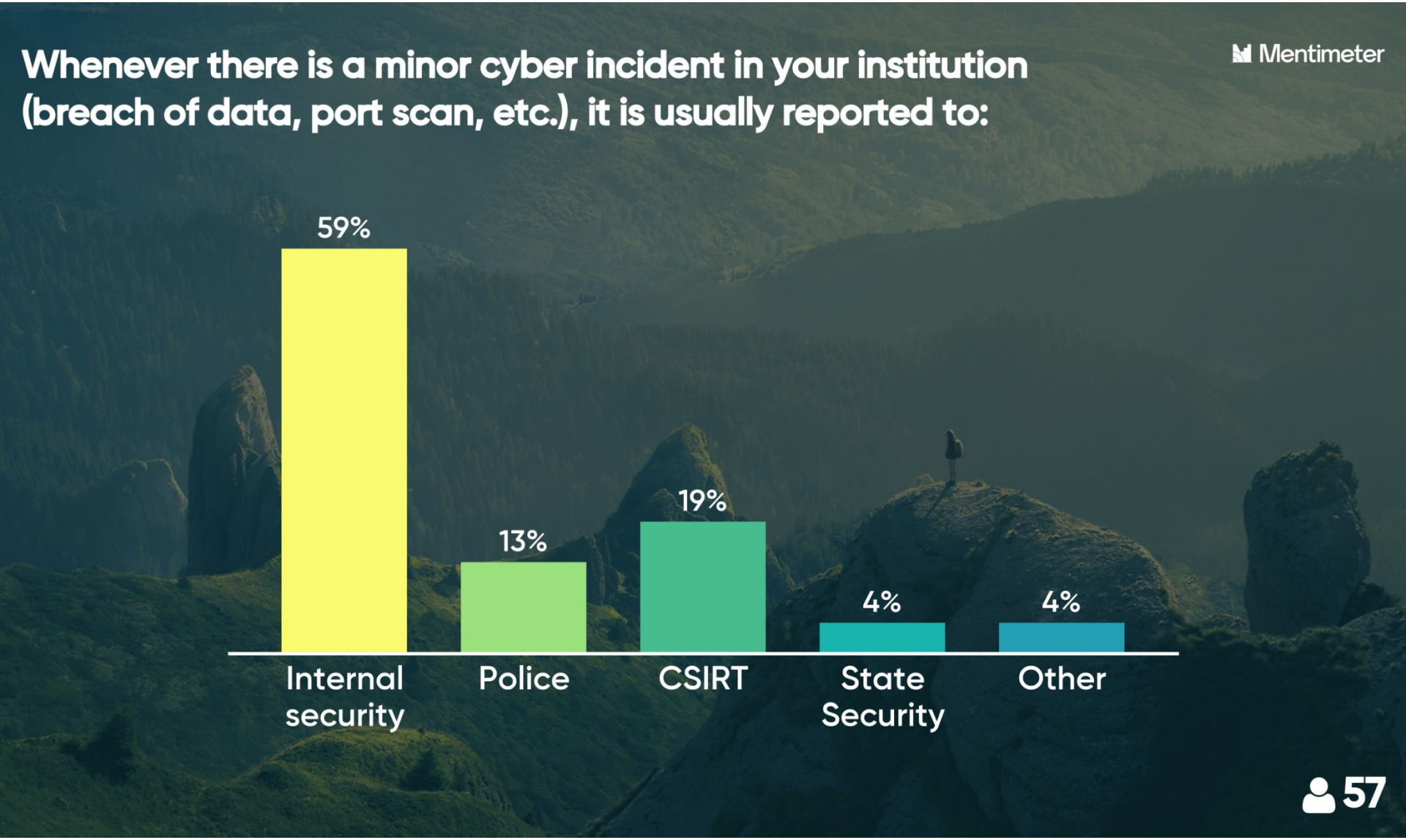
- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

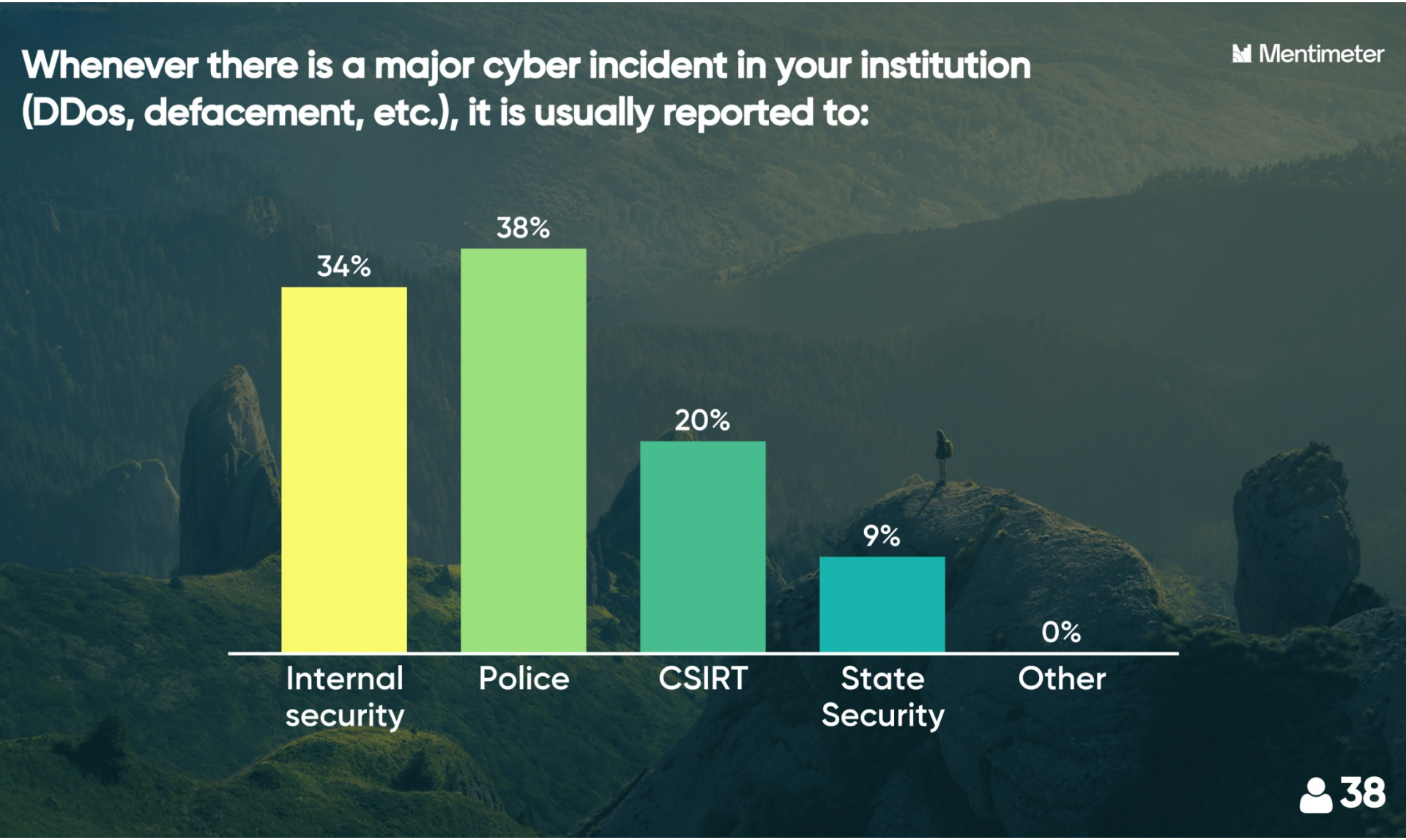
Harmonisation


Your view on current level of cooperation between law enforcement and CSIRT/CERT
Mentimeter
1
7
25
9
28
It is working well
Not working at all
Working but requires significant imporvement
Working but requires slight imporvement
Not sure
70

Are we speaking the same language?

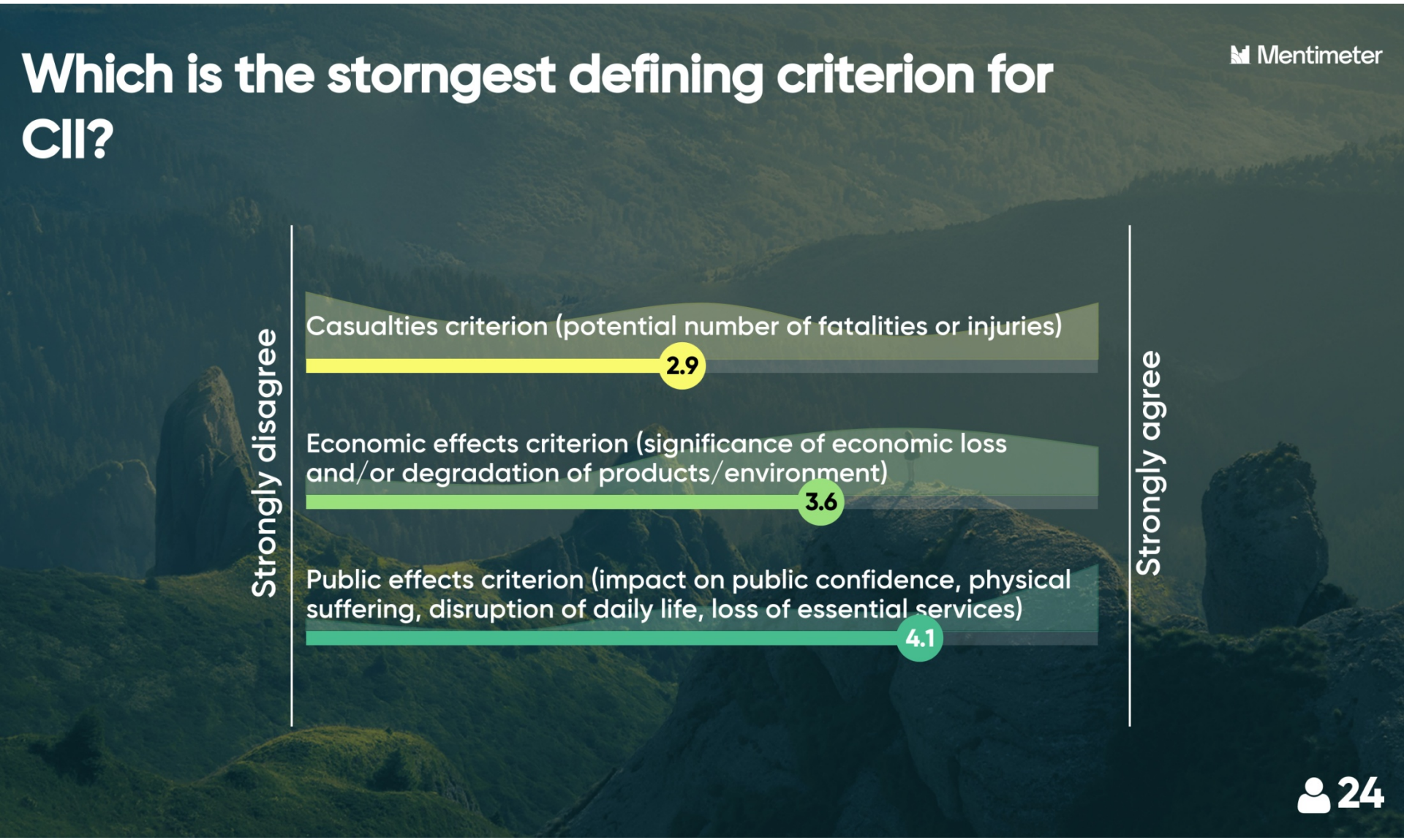
- **Main question**: cybersecurity incident to be handled or criminal offence warranting investigation?
- One incident, **several paths** to follow (internal, CSIRT/CERT, law enforcement, other agency, etc.);
- Define what is the **scope** of incident handling: prevention, report, management, corrective action;
- Time of **discovery**/first response route is important;
- Applicable **framework** can often dictate the fate of incident vs. case;
- **Who** is entitled to define the act as "incident" or "crime"?
- Common **Taxonomy** for Law Enforcement and the National Network of CSIRTs:
  - Produced jointly by ENISA / Europol, actual version 1.3 December 2017
  - Mapping each type of cyber incident with relevant international legal framework


Whenever there is a minor cyber incident in your institution (breach of data, port scan, etc.), it is usually reported to:
Mentimeter
59%
13%
19%
4%
4%
Internal security
Police
CSIRT
State Security
Other
57


Whenever there is a major cyber incident in your institution (DDos, defacement, etc.), it is usually reported to:
Mentimeter
34%
38%
20%
9%
0%
Internal security
Police
CSIRT
State Security
Other
38

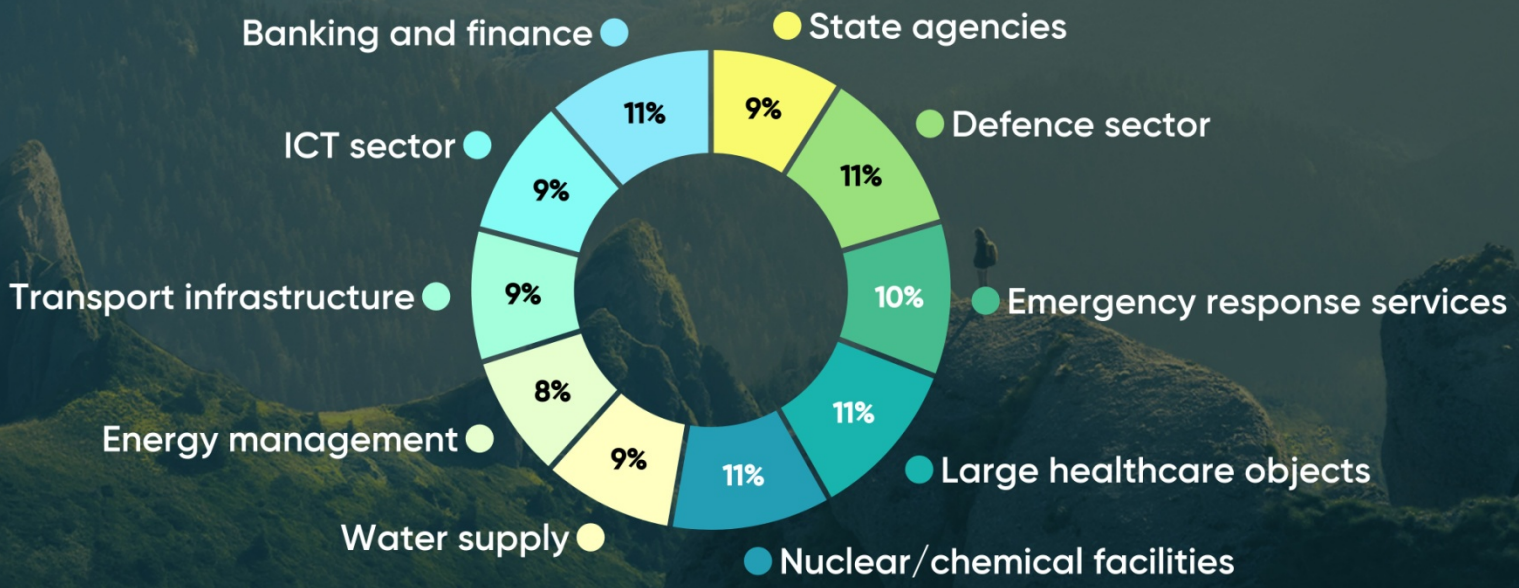
What is critical infrastructure?

- Infrastructure should be **critical**: no one-fits-all approach;
- No possibility for any state to accord the same level of protection to all infrastructures: criticality is a defining factor for allocating **resources**;
- Protection of CII does not mean response **only** through ICT;
- Defining infrastructure through **common sense** is tempting, but runs against the principles of proper management and security;
- The EU approach is exemplary for reasons of future integration, but also in terms of evolution through debate and research (e.g. **criteria** of casualties, economic effects and public effects since 2008);
- Identification and protection of CII still remains a **national matter**;
- The identification of CIIs for protection is less problematic for state agencies, but far more challenging in terms of **private entities**.


Which is the storngest defining criterion for CII?
Mentimeter
Strongly disagree
Strongly agree
Casualties criterion (potential number of fatalities or injuries)
2.9
Economic effects criterion (significance of economic loss and/or degradation of products/environment)
3.6
Public effects criterion (impact on public confidence, physical suffering, disruption of daily life, loss of essential services)
4.1
24

Mentimeter

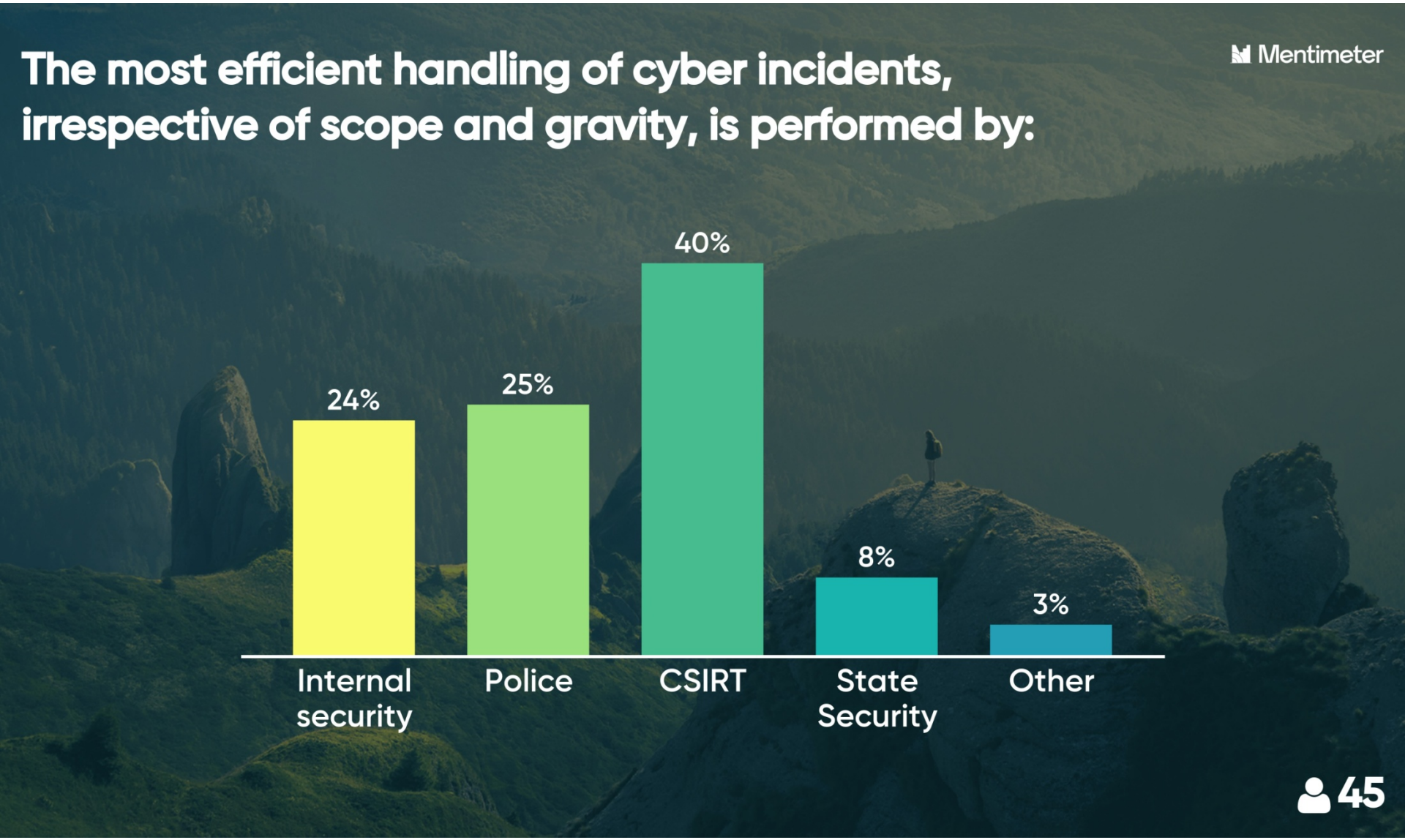
Please rate these services in terms of critical value and effect on cybersecurity



30

How much effort/resources are required?

- The "**1% problem**": only 1% of all reported incidents/crime would end up in criminal convictions;
- Relative lack of **regulation** in cybersecurity domain but strong safeguards and detailed regulation in the criminal justice domain;
- Criminal justice process is more time- and **resource**-consuming;
- Less **oversight** agencies (e.g. courts) who would evaluate the admissibility of evidence in cases of CSIRT handling of incidents;
- **Capacities** of police agencies to deal with incidents reported as criminal cases;
- **Disparity** of skills, pay grade and career growth between criminal justice and cybersecurity sector;
- There are less formalities for CSIRT **cooperation across borders** compared to criminal justice (e.g. MLA).


The most efficient handling of cyber incidents, irrespective of scope and gravity, is performed by:
Mentimeter
24%
25%
40%
8%
3%
Internal security
Police
CSIRT
State Security
Other
45

Octopus Conference 2019, Workshop 3: Selected suggestions from the audience

- ✓ COMPLETE MERGER/FUSION OF THE CSIRT/LEA.
- ✓ To increase efficiency and productivity need more **human and financial resources**.
- ✓ Better sharing of information, talking the same language, improved frameworks for cooperation, **increased trust.**
- ✓ Harmonization of standards, establishment of cooperation networks, **information sharing in relation to multi-jurisdictional attacks**, collaboration between law enforcement agencies within different states.
- ✓ **Secondment** of personnel (for specific periods) from the national CSIRT to law enforcement and vice versa / Exchange Human Resources among the institutions involved.
- ✓ Having Law Enforcement detached **agents** in CSIRT.
- ✓ Share information, more practices on using **informal channels** but within the legal borders or frameworks. Establishing a good relationship to have better outcomes. **Relationship first, outcome second**.
- ✓ Better **understanding of the issues** and continuous collaboration amongst member countries in the way forward in fighting cybercrime.
- ✓ Clear roles and responsibilities defined in a **Standard Operating Procedure.**
- ✓ **Capacity building**, awareness and sharing of information among all stakeholders.

Capacity building example: Cyber Resilience in the Eastern Partnership

- **Source**: Action Document for EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries
- **Challenge**: Sharing of relevant data held by CSIRTs on incidents and attacks with all concerned authorities: information sharing most valuable to law enforcement and judicial authorities.
- Without this cooperation, it is difficult to determine the **scale** and **trends** of cybercrime and **threats** to cybersecurity and thus to inform cybercrime and cybersecurity **strategies**.
- Thus, two interconnected components:
  - Development of technical and cooperation mechanisms that increase **cybersecurity** and preparedness to cyber-attacks, such as functional CSIRTs, table-top exercises and improving cyber hygiene.
  - Capacities to fight **cybercrime** and enable access to **electronic evidence**, including compliance with Budapest Convention, improving operational capacities of cybercrime units, strengthening interagency, international and public/private cooperation.

CyberEast Objective/Outcome 2
Improving capacities and interagency cooperation

Immediate Outcome 2 of the project seeks to reinforce the capacities of judicial and law enforcement authorities and interagency cooperation, seeking to encompass all criminal justice stakeholders in the EaP countries into coherent, sustainable and skills-oriented experience sharing and training framework.

To achieve this, the Outputs under this Outcome aim at:

- Strengthening skills and institutional setup of operational cybercrime units in law enforcement authorities.
- **Improving interagency cooperation of relevant law enforcement and criminal justice authorities, agencies and bodies including through improved data sharing.**
- Internal and external accountability and oversight including role of civil society organisations reinforced.
- Improved public communication and transparency on cybercrime actions.
- Reinforce mechanisms for trusted cooperation between the private sector, citizens and criminal justice authorities.

CyberEast Project
Relevant / planned activities 2020-2022

- Yearly **Regional Cyber exercises** to improve interaction between CSIRTs and law enforcement agencies in real-time environment.
- Support to **national cyber exercises** with cybercrime and cybersecurity institutions.
- Support to **cooperation forums** and meetings for networking between cybercrime and cybersecurity professional communities.

- Support to organization of national and regional Internet industry and **technology events** increasing trust between the public, the state and the private sector in ensuring security of cyberspace.
- Business analyses and development of **agreed procedures** for cybercrime/incident reporting and sharing of data by (CSIRTs) with criminal justice authorities – through country-specific workshops with regional conclusions.
- Assessment of efficiency of cybercrime **reporting systems**.

Thank you for your attention

Giorgi Jokhadze
Project Manager
Cybercrime Programme Office
Council of Europe - Conseil de l'Europe
Bucharest, Romania
Giorgi.Jokhadze@coe.int