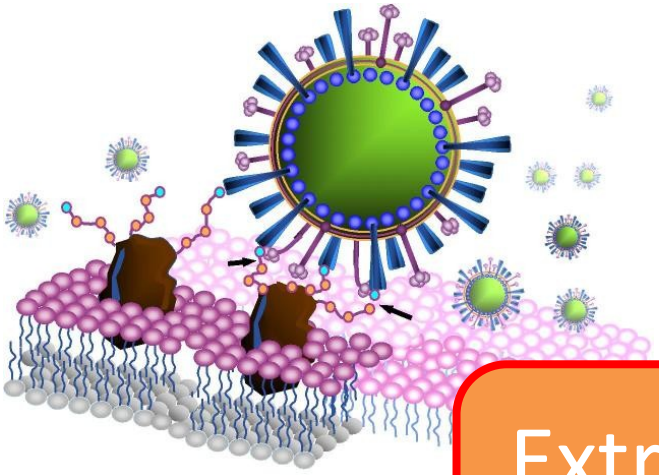
EGI - Identity Management

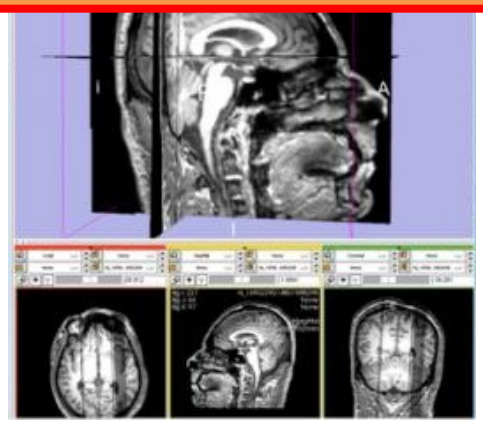
Steven Newhouse
Director, EGI.eu

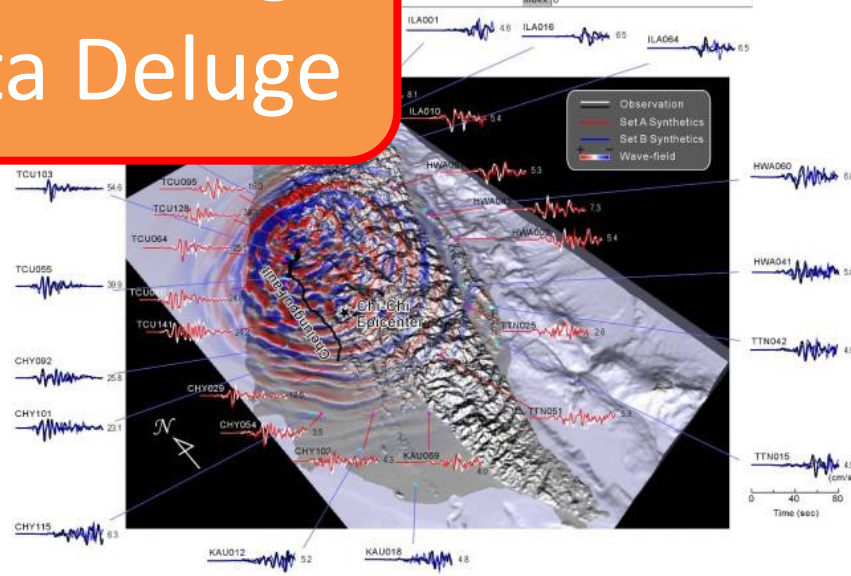
e-infrastructure

C21: Digital Research



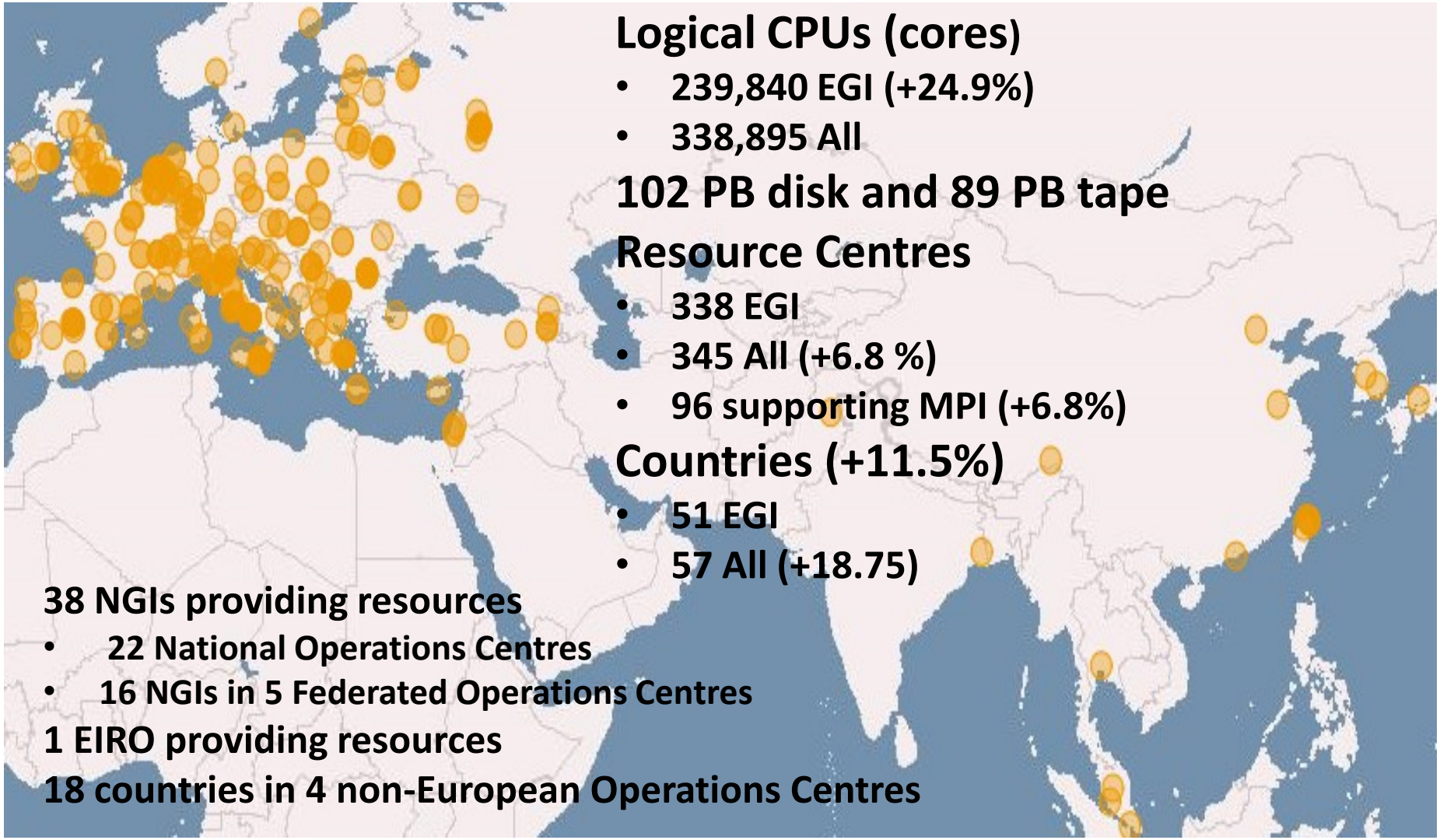
Extracting Knowledge from the Data Deluge





European Grid Infrastructure

(April 2011 and yearly increase)



Logical CPUs (cores)

- 239,840 EGI (+24.9%)
- 338,895 All

102 PB disk and 89 PB tape

Resource Centres

- 338 EGI
- 345 All (+6.8 %)
- 96 supporting MPI (+6.8%)

Countries (+11.5%)

- 51 EGI
- 57 All (+18.75)

38 NGIs providing resources

- 22 National Operations Centres
- 16 NGIs in 5 Federated Operations Centres

1 EIRO providing resources

18 countries in 4 non-European Operations Centres

Conflicting Issues

- Federated Pan-European Infrastructure
  - Need to deal with local laws & processes
  - Complex as part of a global collaboration

  →Resource access needs to managed
- Support multi-disciplinary user communities
  - Each community has different operating models
  - Different levels of technology expertise & use

  →Resource access tuned to the community

Key Points

- Authentication token needs to be trusted
  - Requires auditable procedures to give value
    - e.g. X.509 CA in the EUGridPMA & IGTF
- Attributes need to be trusted
  - Based on the individual, e.g. staff/student
  - Based on their community e.g. VO membership VOMS
- Authorisation separated from authentication
  - Performed locally for each service, e.g. ARGUS
- Agreed common policies underpin technology

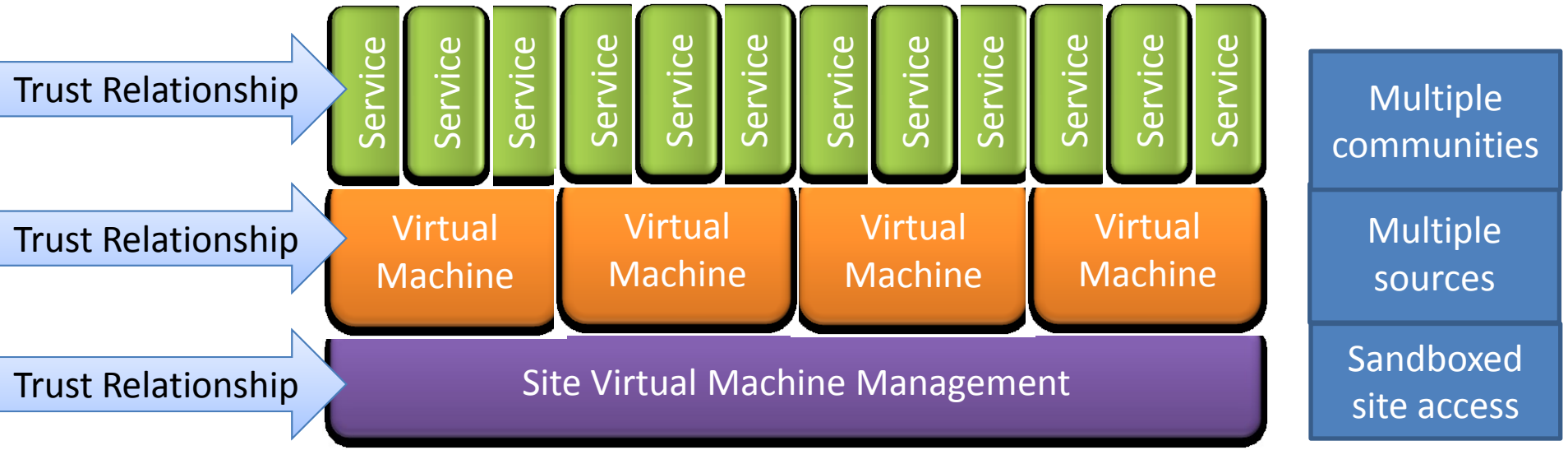
Non-Proliferation Issue

- Major concern for the EGI Council
  - Local interpretation of international laws
  - Compliance needs to be demonstrated

- **Need**: Nationality Attribute
  - No attribute → may mean no access

Future Challenges

- Virtualisation changes the relationships



- Multiple trust relationships
- Multiple trust levels

Implementation

- Global interoperability is essential
  - e.g. X.509, Kerberos, SAML, …
- Link quality of attribute to authorisation
  - e.g. photo ID linked to IGTF X.509 certificate
  - e.g. verified email address linked to login
- Ease of use critical to wider adoption
  - e.g. short-lived certificate servers, security token servers

    → Convert ‘normal’ ID tokens to ‘Grid’ tokens

Conclusions

- Virtualisation changes the game
  - Can separate management from use
- Security of the whole infrastructure critical
  - Traceability across different tokens key
- Need solutions with global scope
  - Either deployment or interoperability

- Contact: director@egi.eu