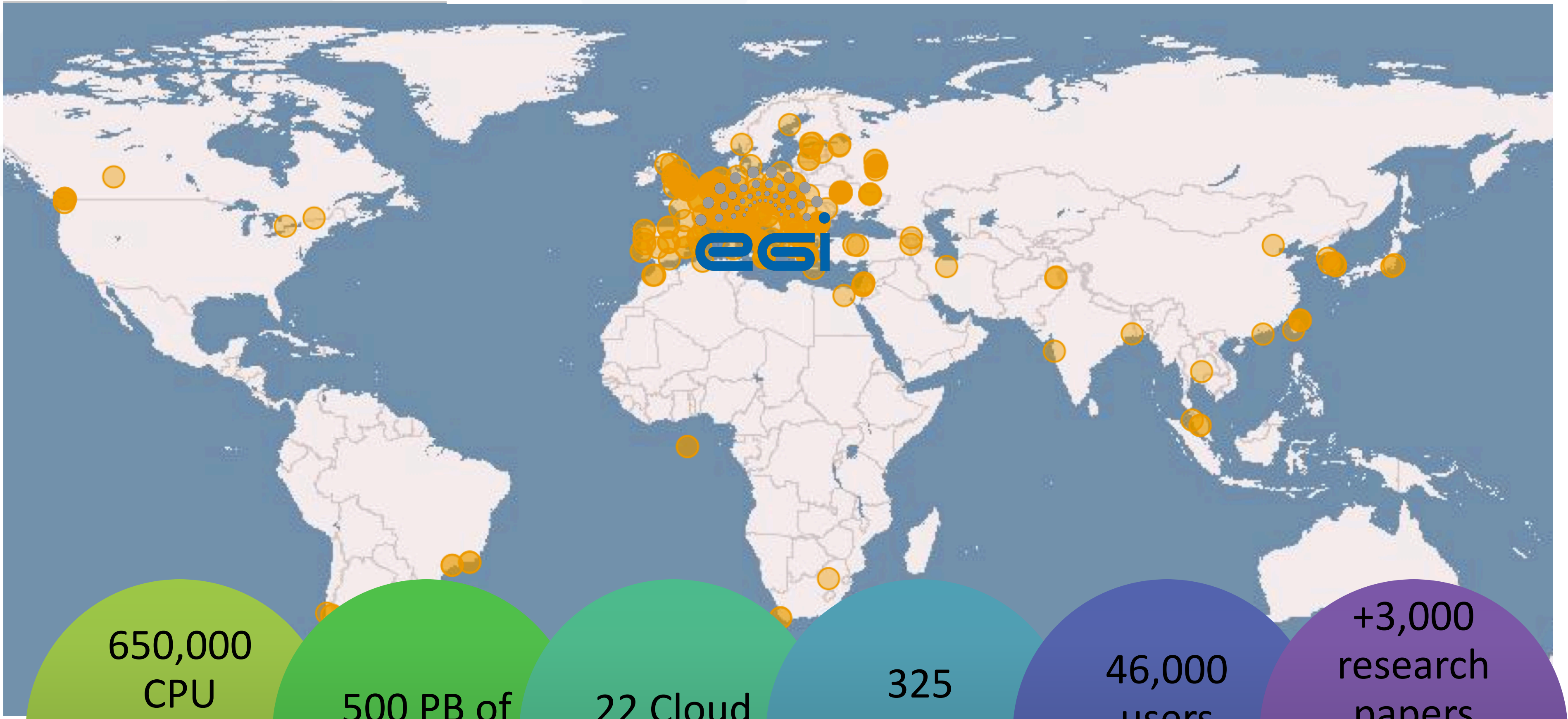
EGI Security
at WISE, XSEDE16, Miami
18 July 2016

David Kelsey (STFC-RAL)

Chair EGI Security Policy Group

www.egi.eu

EGI federated infrastructure, QR1 2016



650,000 CPU Cores

+23.6%

500 PB of storage

22 Cloud providers

325 resource providers

46,000 users

+21%

+3,000 research papers

> 780 in 2016

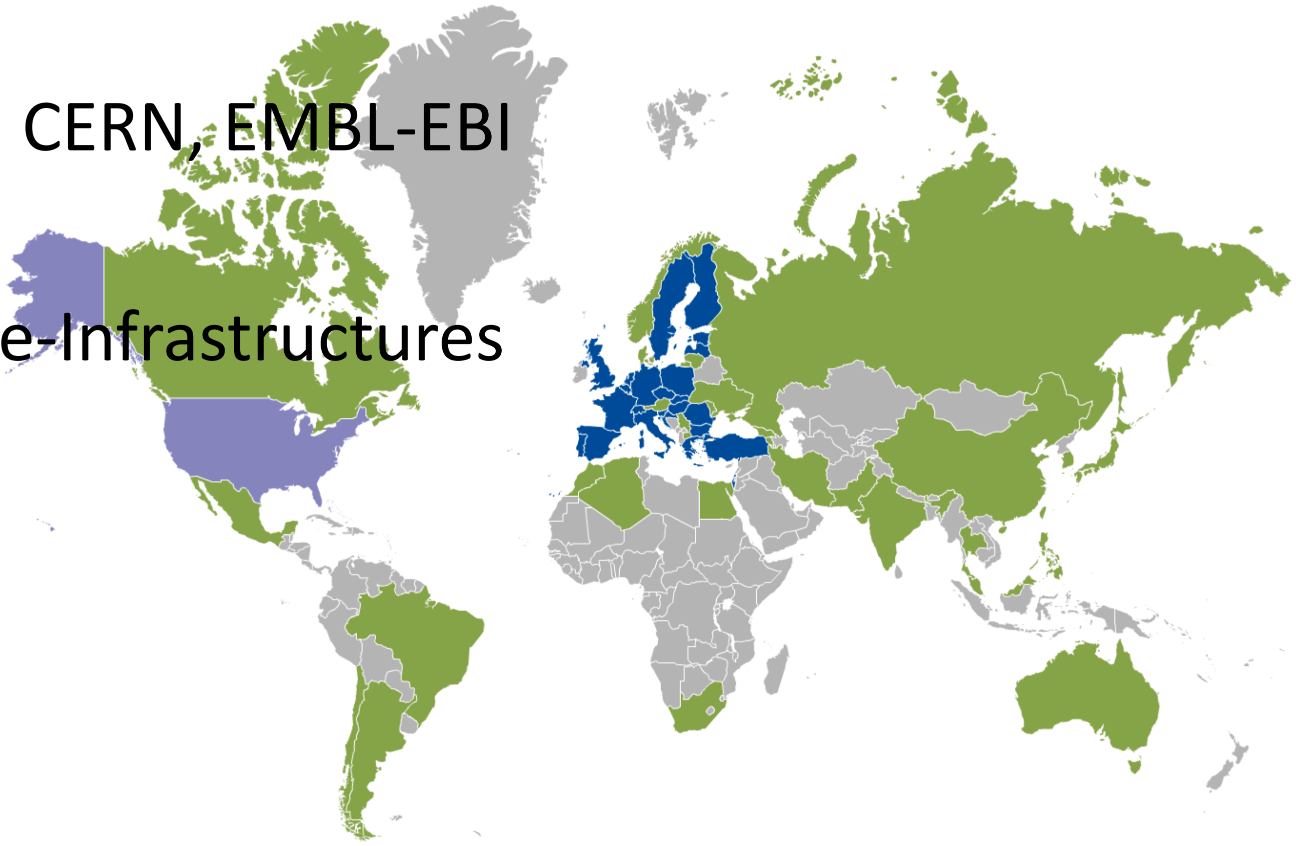
A system of open e-Infrastructures

🟥 58 countries worldwide

🟦 EGI: 22 NGIs, CERN, EMBL-EBI

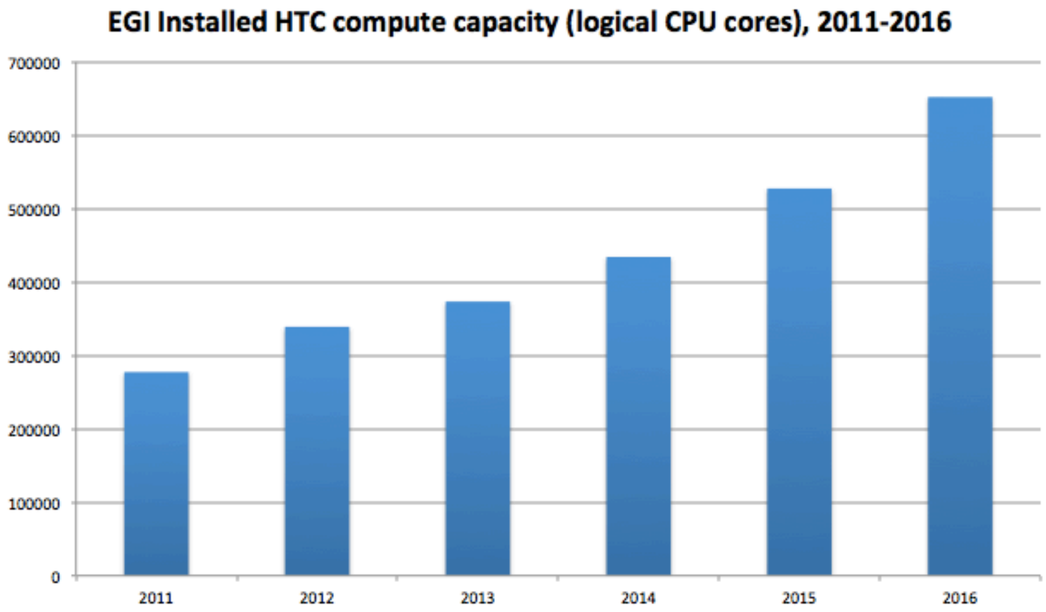
🟩 6 Integrated e-Infrastructures

🟪 1 peer (OSG)



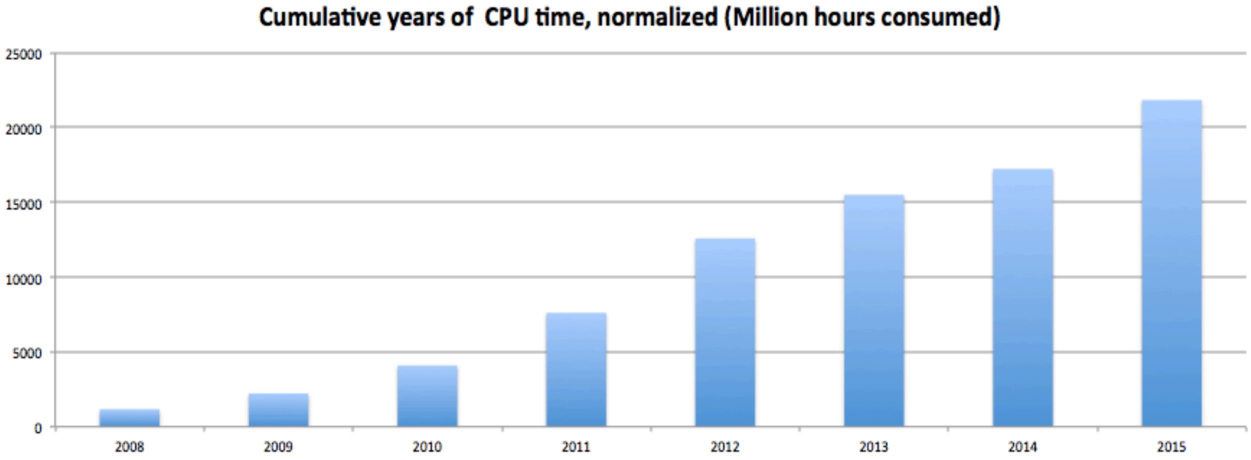
www.egi.eu

HTC installed capacity and consumption 2/2



Installed capacity
2011-2016

650,000 cores



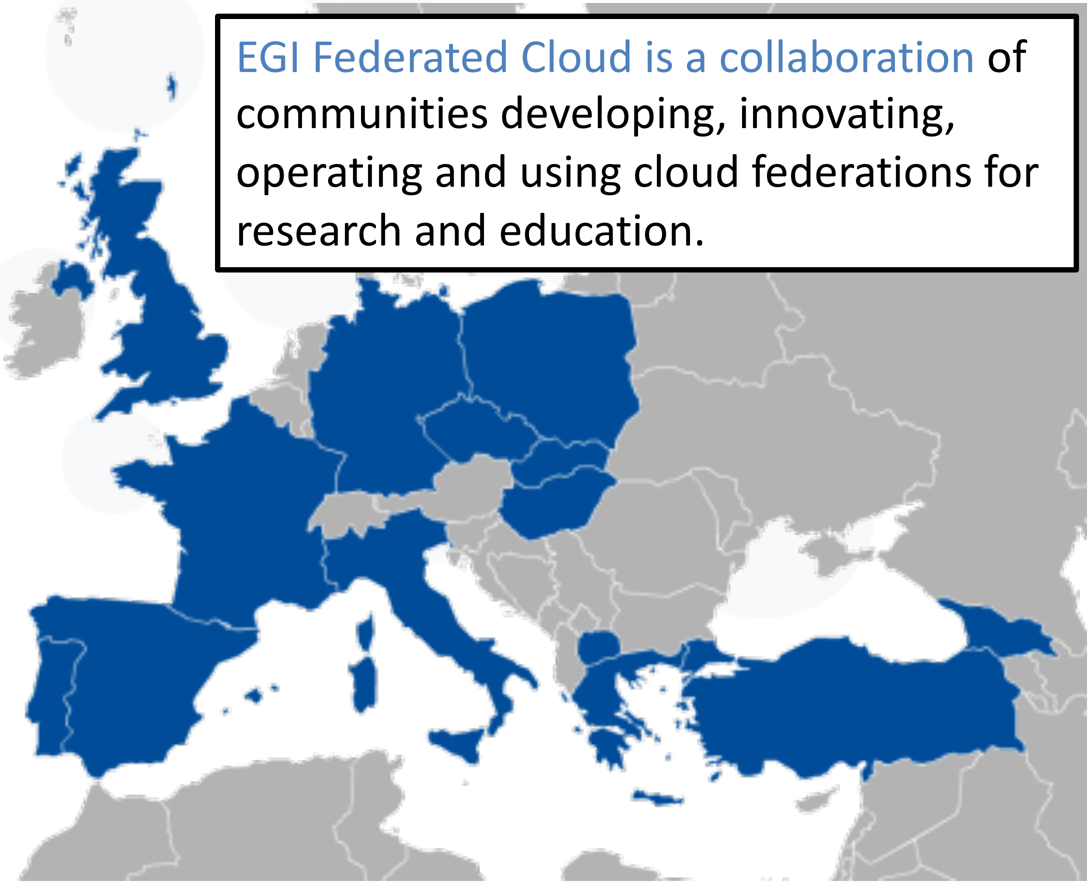
Usage
2008-2015

21 Billion

www.egi.eu

EGI Federated Cloud

EGI Federated Cloud is a collaboration of communities developing, innovating, operating and using cloud federations for research and education.



IPHC Institut Pluridisciplinaire Hubert CURIEN STRASBOURG

CETA Ciemat

MetaCentrum

JÜLICH FORSCHUNGSZENTRUM

TÜBİTAK ULAKBİM

INFN Istituto Nazionale di Fisica Nucleare

CYFRONET

bifi

LIP

Grid y Computación de Altas Prestaciones GRyCAP

Slovak Academy of Sciences

grnet Networking Research and Education

CSIC Consejo Superior de Investigaciones Científicas

Ss. Cyril and Methodius University in Skopje FACULTY OF COMPUTER SCIENCE AND ENGINEERING

100%IT

And now to EGI security

Organisation of EGI Security

- Security Coordination Group (SCG)
- Security Policy Group (SPG)
- Software Vulnerability Group (SVG)
- EGI CSIRT (TI certified)
  - Incident response, monitoring, security challenges, training
- IGTF/EUGridPMA
- Funded by NGIs, EGI.eu, EU H2020 (EGI-Engage)
- A lot of cross-membership
  - Core team of ~ 8-12 people (not all full-time)
- Linked to more general EGI Operations

EGI Security Developments

- Funded by EU H2020 EGI-Engage
- EGI Federated Clouds service
  - New trust model, policies and procedures
- EGI Long Tail of Science service
- Hiding certificates from users
  - Federated login, credential translation, etc
- Addressing different Levels of Assurance
- Last two in collaboration with EU H2020 AARC project

Future

- We already have collaborated well with others
  - Joint training events with EUDAT and PRACE
  - Would like to organise more joint training events
    - E.g. a Federated Identity role-play at DI4R joint with AARC
- Desire for stronger collaboration on incident handling
  - Sharing intelligence and aspects of vulnerability handling
- More on risk assessment, standards, best practices
- Joint bids for future funding opportunities?
- EGI finds the WISE Community to be a great place to do the collaboration

For more technical details

- Sven Gabriel (the EGI Security Officer) gave a nice talk at ISGC2016
  - **EGI-CSIRT: Organising Operational Security in evolving distributed IT-Infrastructures**
  - *Https://indico4.twgrid.org/indico/event/1/session/31/contribution/67*

- A major challenge over the last year or two for the EGI security teams
  - How to we mitigate the identified security risks?
  - EGI Federated Cloud service
  - What is the correct balance of monitoring, control, freedom?
- *Which leads to a proposal for a possible new WISE working group*

www.egi.eu

(Federated) Cloud Security for R&E - a possible WISE WG?

David Kelsey, STFC
at the WISE BoF – TNC16 – 14 June 2016

Federated Cloud Security?

- In the EGI Federated Cloud service (distributed management domain)
  - (Some) user communities have conflicting requirements
    - Any user can start a VM and have full control of the VM (root access)
    - Others want wide open networking to the general internet
      - We have tried to control this via policy (endorsement of VM images, operator requirements)
- This is not good for our security risk assessment!
  - How do we reduce the likelihood and impact of security incidents?
  - And security incidents DO happen
- Commercial Cloud providers
  - Have sophisticated control and monitoring technology
  - Have large security teams (and a single management domain)
  - Have terms and conditions and the customers credit card number!

A possible WISE working group?

- Many in the NREN & e-Infrastructures community are providing Cloud services
  - How do they mitigate the security risks?
- Should we form a WISE working group?
  - To share experiences
  - To jointly document best practices
- What monitoring and control is necessary?
  - Firewalls, sandboxes, audit logs, traceability, network monitoring, …
- What policies (terms and conditions) are needed?

Thank you for your attention.

Questions?