CSIRT Task Force: Cooperation in Europe

Andrew Cormack
A.Cormack@ukerna.ac.uk
Don Stikvoort
Don.Stikvoort@s-cure.nl

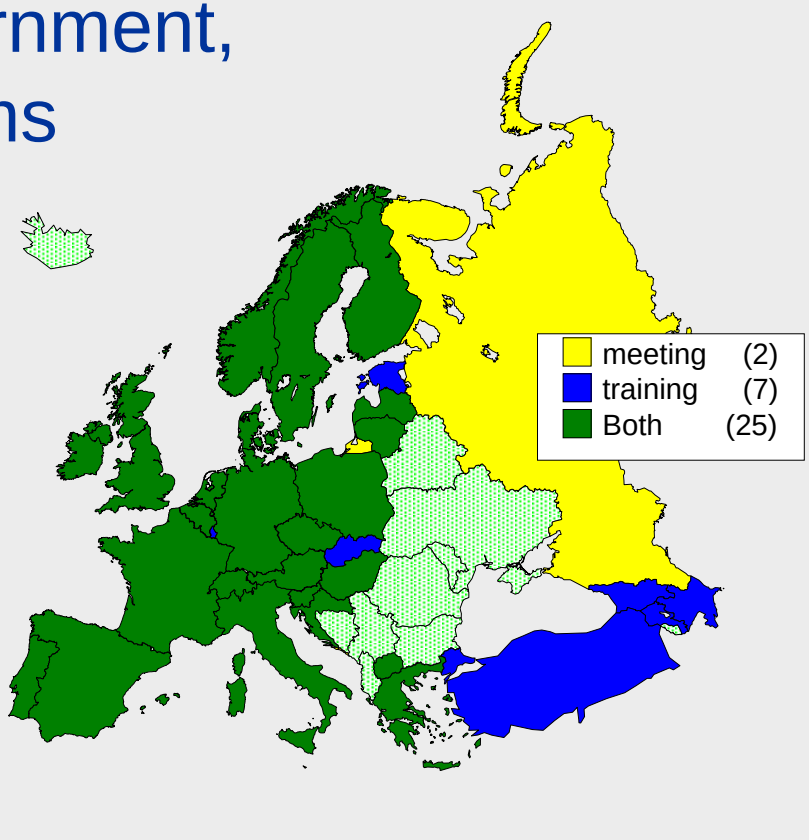
Based on materials provided by TERENA TF-CSIRT

How it works

- Three meetings a year since 2000
  - Following meetings/projects since 1993
  - Open to those working in incident response
  - Sharing knowledge, building trust
  - All results published or freely licensed
- Rotating volunteer host organisation
- TERENA provides secretariat
- Subgroups propose R&D projects
- Trust promotes operational cooperation

Who is involved?

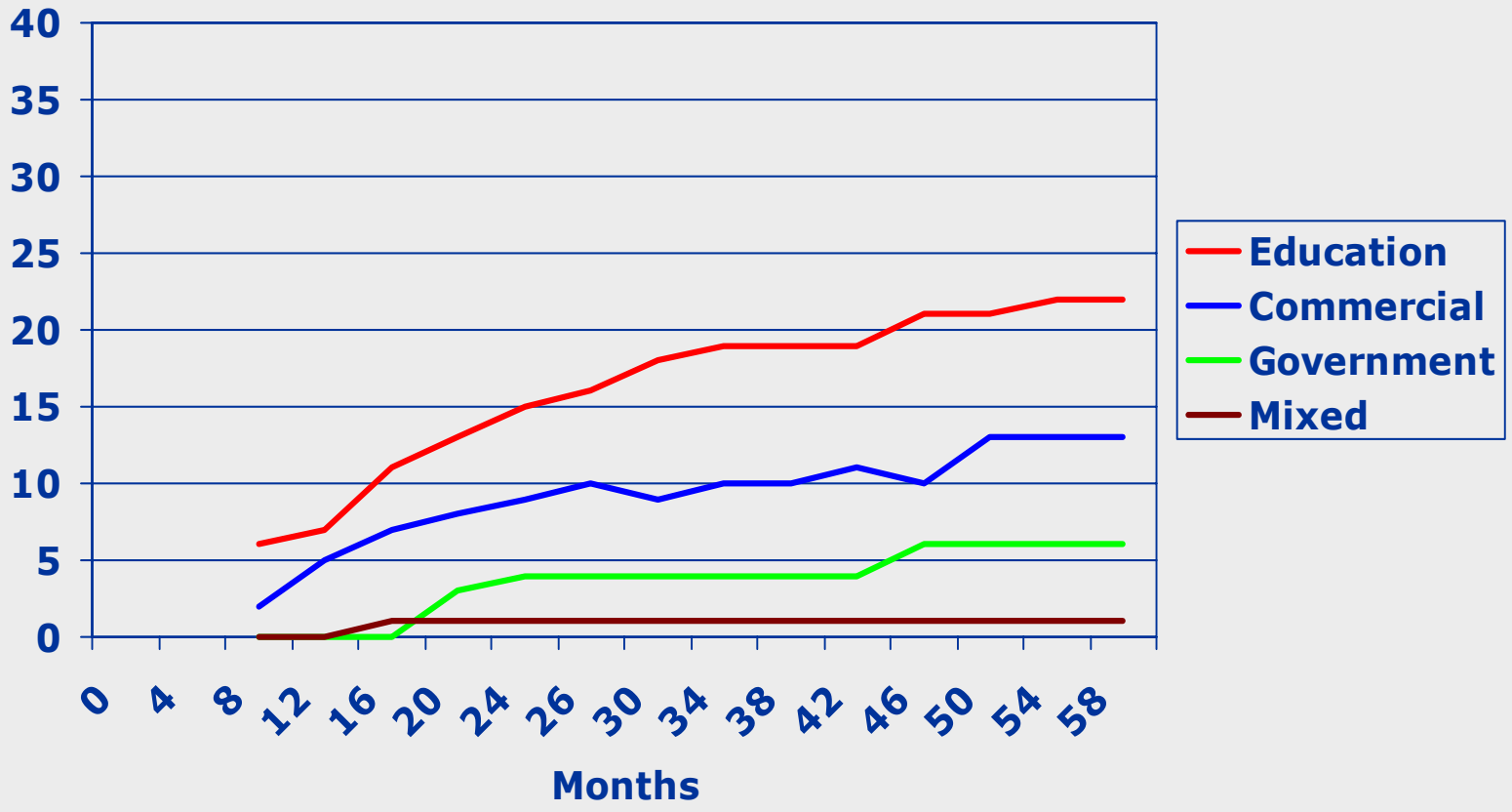
- Academic, Government, Commercial teams
- 34 countries



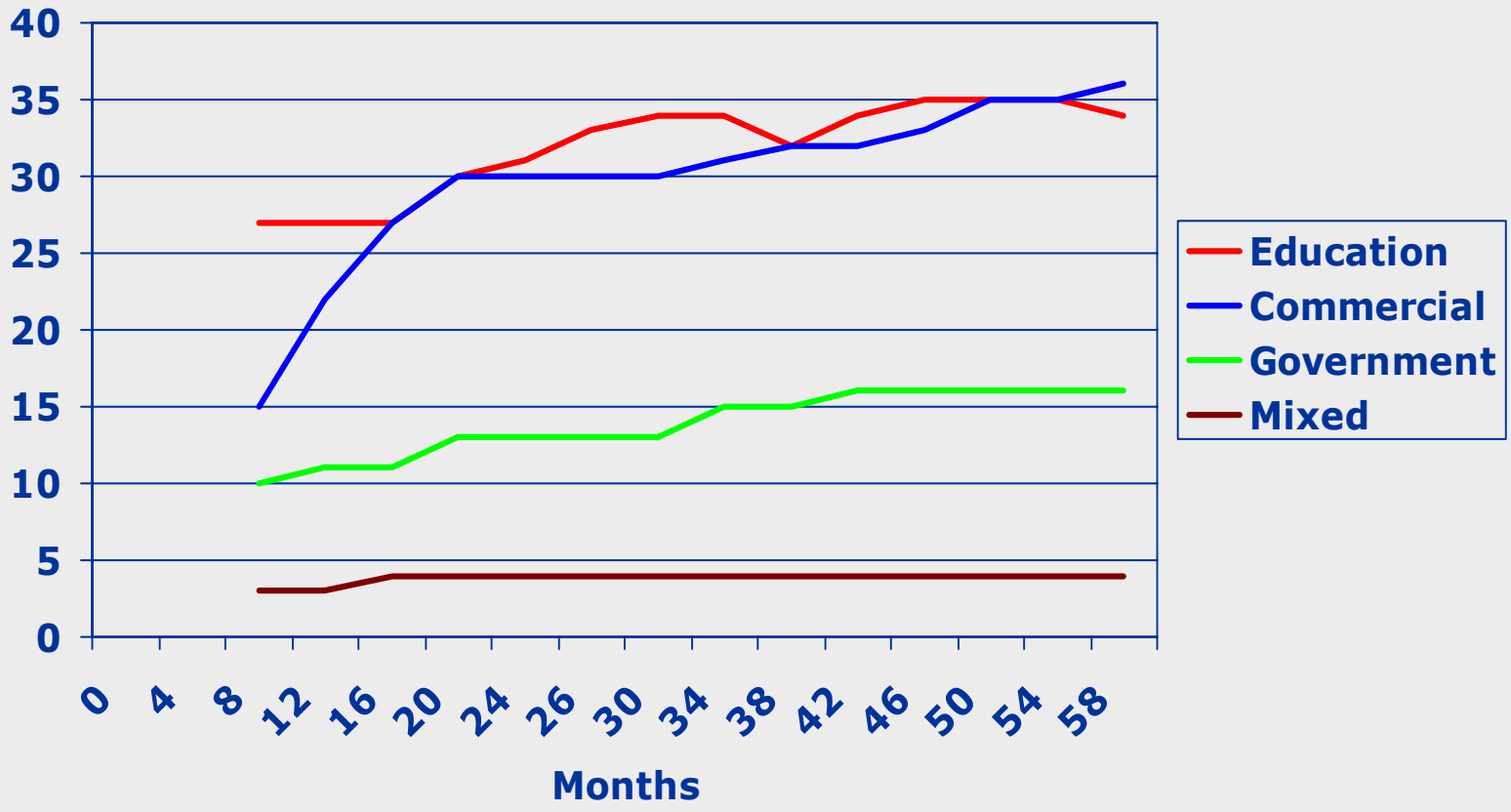
Building trust – TI

- Need trust before sharing sensitive data
  - Incident response, alerting, etc.
- So accredit teams who
  - Define their operational parameters
  - Conform to best practice
  - Maintain up to date information
- Checks made by independent 3rd party
- Provides basis for team/team trust

TI Accredited Teams



TI Known Teams



TI services/projects

(Activities that require strong trust)

- Directory of CSIRTs
- Incident information exchange
- Incident handling procedures
- In-band and out-of-band alerting
- Sensor network for scans/incidents
- eCSIRT.net project (FP5)

Task Force projects

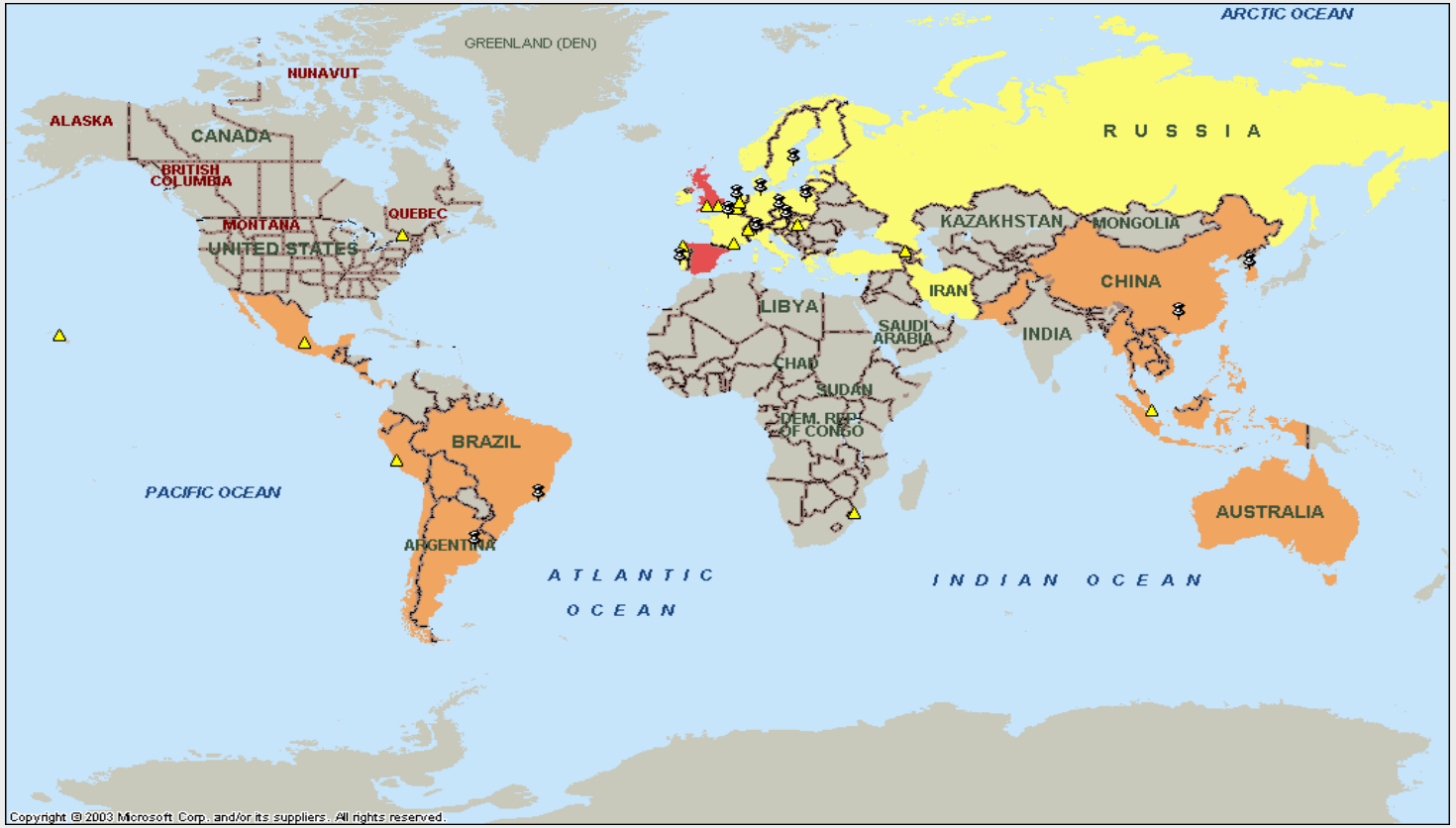
(Activities needing common interest)

- IODEF (exchange of incident descriptions)
  - Adopted by anti-phishing community
- RIPE IRT object (“find the CSIRT”)
- Directory of Incident Handling Tools
  - Information about tools used by the community
- TRANSITS training course
  - Training new staff and new CSIRTs
- Incident Tracking software
  - Commercial quality, open source license
- Vulnerability Information Exchange

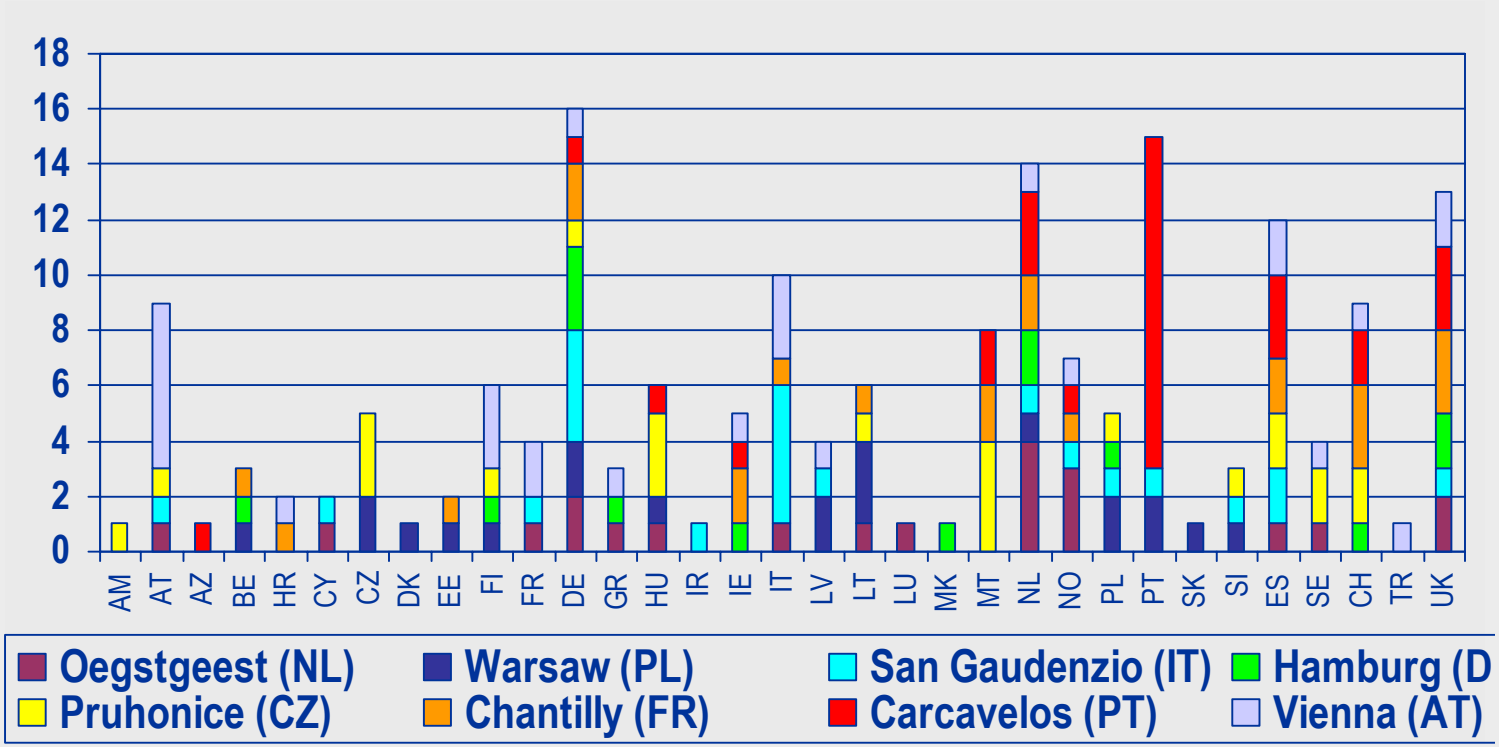
TRANSITS training course

- Materials developed by TF members
  - Intensive, 2 day course on CSIRT essentials
  - Courses delivered by community members
  - Teaching, discussion, trust-building
- EC (FP5) funded delivery from 2002-5
- Now self-sustaining in Europe
  - National and international presentations
  - Assisted by ENISA
- And being exported world-wide
  - Maintenance/management by TERENA & FIRST

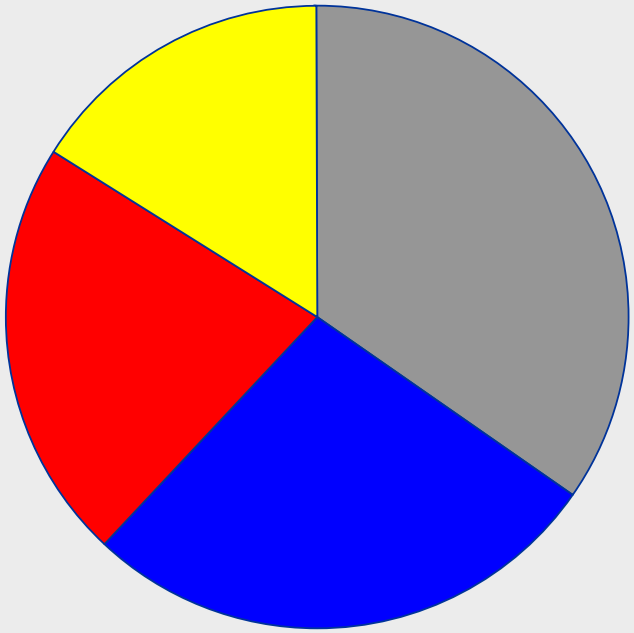
TRANSITS students



TRANSITS in Europe



TRANSITS by sector



Conclusions

- Highly effective cooperation
  - For both operational and R&D tasks
- Spin-offs from original model
  - Europe: EGC, e-COAT
  - Asia-Pacific: APCERT
  - Latin America: CLARA
- Still lots to do, working with ENISA
  - To promote take-up of existing work
    - Only 25% of EU Internet has a CSIRT or Abuse Team
    - ENISA working group identifying gaps
  - To identify new R&D work areas