



CSIRT Task Force: Cooperation in Europe

Baiba Kaskina

Baiba@latnet.lv

Andrew Cormack

A.Cormack@ukerna.ac.uk

Based on materials provided by TERENA TF-CSIRT



International Groups

- TF-CSIRT (<http://www.terena.nl/activities/tf-csirt/>)
 - European CSIRT collaboration
 - Open to those who want to improve incident response
- ENISA (<http://enisa.europa.eu/>)
 - EC advisory agency on Network and Information Security
- FIRST (<http://www.first.org/>)
 - Worldwide CSIRT forum
 - Established teams only (but conference is open to all)
- APCERT (<http://www.apcert.org>)
 - Asia-Pacific CSIRT collaboration
 - Operational group of national level CSIRTs



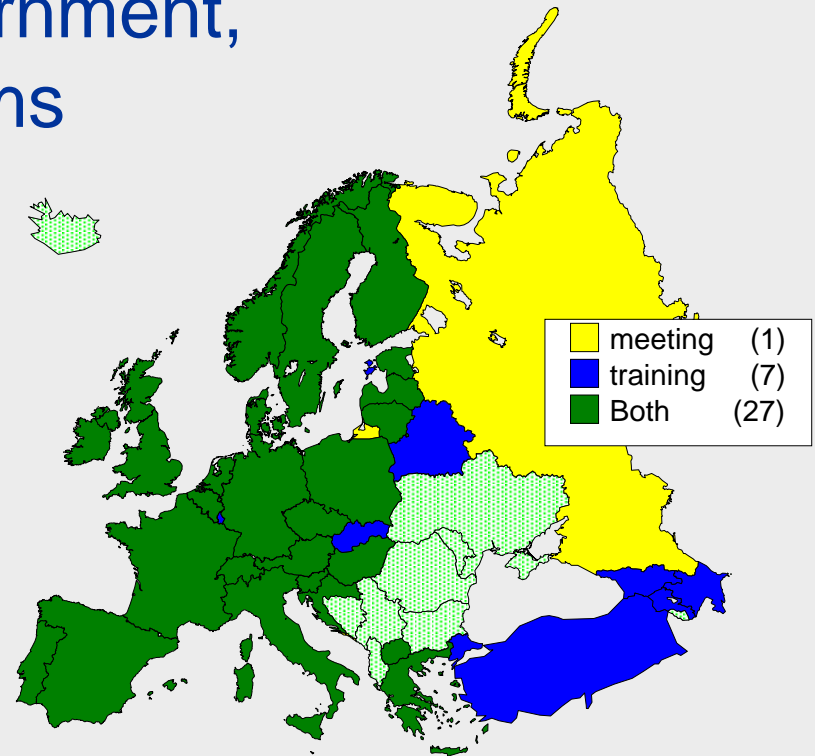
How TF-CSI RT works

- 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
- 35 countries





Helping Teams to Form

- CSIRT starter kit
 - List of Frequently Asked Questions and Answers
 - <http://www.terena.nl/activities/tf-csirt/starter-kit.html>
- Directory of Incident Handling Tools
 - Information about tools used by the community
 - <http://chiht.dfn-cert.de/>
- TRANSITS training course
 - Training new staff and new CSIRTs
 - <http://www.ist-transits.org/>
- CSIRT mentoring
 - Putting existing and new teams in touch
 - <http://www.terena.nl/activities/tf-csirt/mentoring.html>



Helping Teams to Work

Operational Activities

- RIPE IRT object (“find the CSIRT”)
- Incident Tracking software (RTIR & AIRT)
 - Commercial quality, open source license

Research activities

- IODEF
 - Format for exchange of incident descriptions
 - Adopted by anti-phishing community
- Vulnerability Information Exchange
 - Identifying what standards exist or are needed



Building trust – TI

- Need trust before sharing sensitive data
 - For 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
- <http://www.ti.terena.nl/>



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)

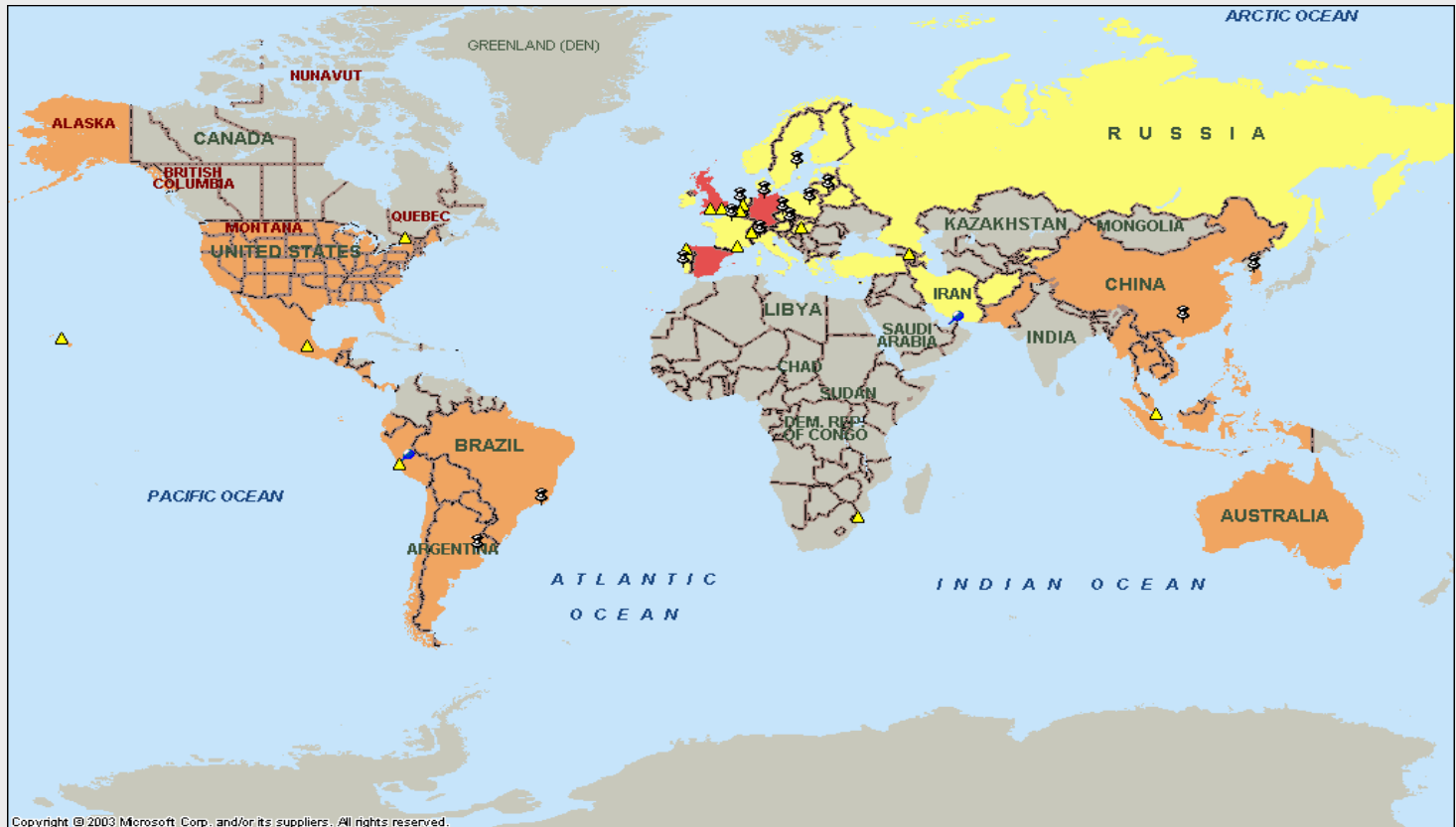


TRANSITS training course

- 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





How To Get Involved

- Come to meetings
 - Next is in Espoo (Helsinki),
September 21-22
- Join the mailing list
 - tf-csirt@terena.nl
 - Need to be sponsored by an existing member

