



GÉANT2 Security (JR2): Transition to Service

Christoph Graf, SWITCH

3rd GÉANT2 Technical Workshop

Cambridge, 10 January 2007



Connect. Communicate. Collaborate

Overview

- When is security (becoming) an issue?
- Risks in the NREN environment and the role of CERTs
- JRA2 recommendations
- JRA2 roadmap in Years 3+4

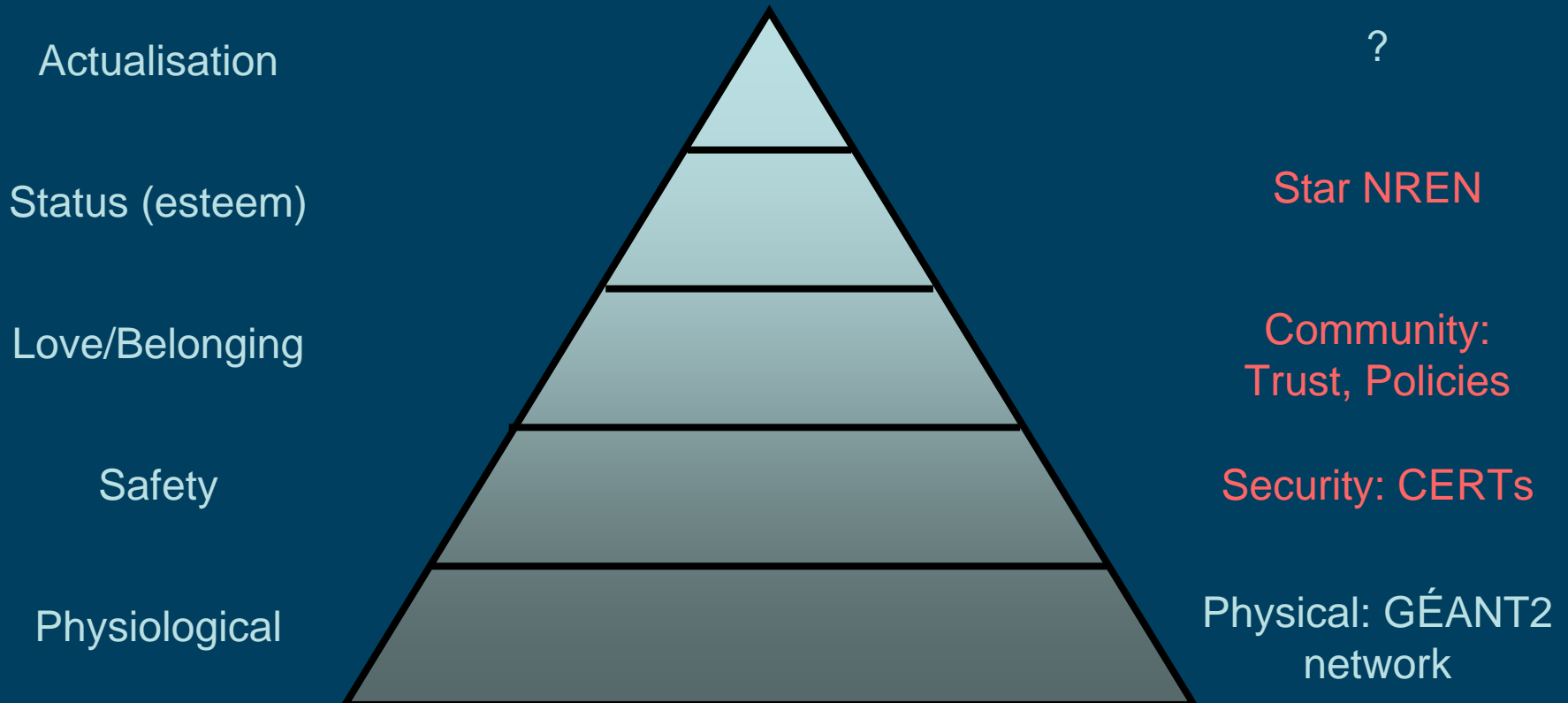
Maslow's Hierarchy of Human Needs



Connect. Communicate. Collaborate

Humans:

NRENs:



Source: <http://en.wikipedia.org/wiki/Maslow>



Connect. Communicate. Collaborate

Risks (I)

Andrew Cormack, UKERNA, at Grid Security 2002:

“What excites hackers?”

- High profile targets – to enhance their reputation*
- Powerful CPU – for password cracking etc.*
- Large disk – to distribute illegal material*
- High bandwidth – for denial of service attacks*
- Valuable files – for espionage or sale”*



Connect. Communicate. Collaborate

Risks (II)

4 Years later... New (additional) question:

What excites criminals?

- The network became a commodity for everybody
- No surprise: “everybody” includes (organised) crime
- Criminals meet on the net risk-unaware users and low-risk law enforcement

-> Good business opportunities!



Connect. Communicate. Collaborate

Risks (III)

- In their role as network operators, GÉANT2 partners are primarily exposed to (may change over time):
 - availability and image
- CERTs role in GÉANT2 partners' risk management:
 - keep up-to-date on underground activity patterns
 - improve risk-awareness of users and management
 - learn to fight symptoms with technical measures
 - reduce the risks to service within the GÉANT2 community, if properly managed



Connect. Communicate. Collaborate

Security Recommendations

- GÉANT2 partners **MUST**:
 - Operate a “recognised” CERT team
 - Basic operational requirements
- GÉANT2 partners **SHOULD**:
 - Additional documentation about the team (BCP)
 - Extra operational requirements
- GÉANT2 partners **MAY**:
 - Use “The Toolset”

MUST Recommendation Summary



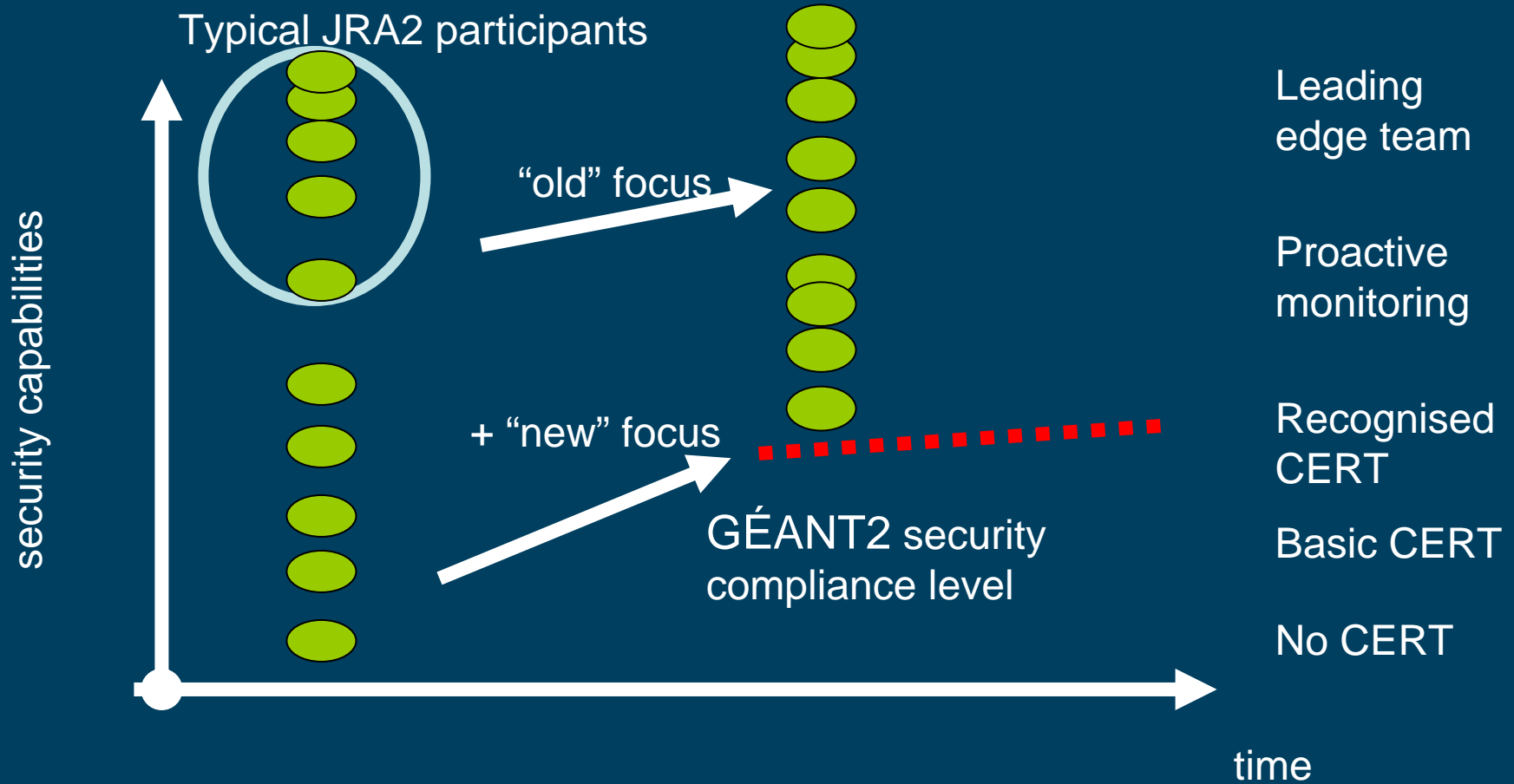
Connect. Communicate. Collaborate

- Recognition
 - Accreditation with the Trusted Introducer on level “Accredited”
- Communication
 - Pre-authenticated PGP keys made available
 - Sensitive information gets proper protection
- Operational requirements
 - Observe information disclosure policy of information source
 - Timely acknowledgement of incoming partner CERT requests and provide status information
 - Appropriate preservation of relevant references (Trouble Ticket IDs) throughout the incident lifecycle
 - ...



Connect. Communicate. Collaborate

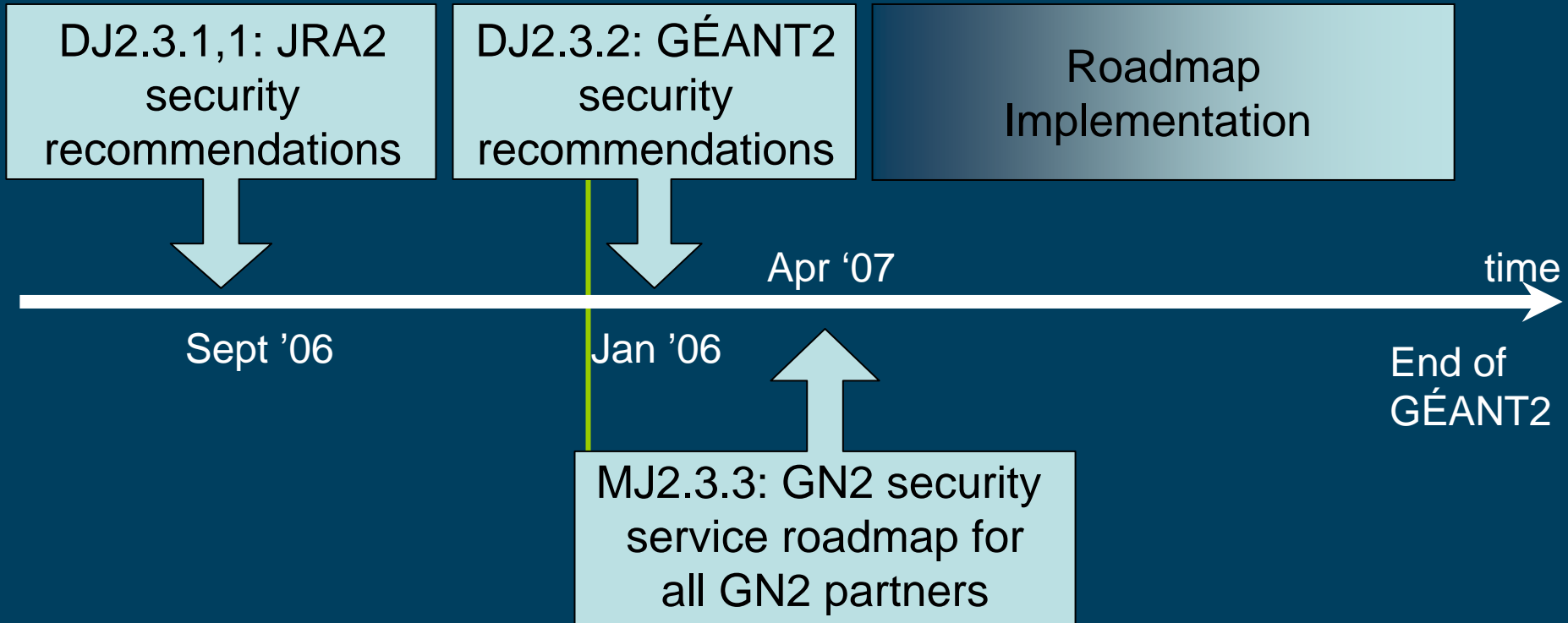
JRA2 (Security) in Year 3+





Connect. Communicate. Collaborate

Roadmap



GÉANT2 NREN Partner Status



Connect. Communicate. Collaborate

- Accredited with the Trusted Introducer: 18
ACOnet, ARNES, BELNET, CARNet, DFN, FCCN, Funet, GARR, GRNET, LITNET, RedIRIS, RENATER, SUNET, SURFnet, SWITCH, UKERNA, UNI-C, UNINETT
- Security teams in operation: 7
CESNET, CyNet, HEAnet, IUCC, NIIF/HUNGARNET, PSNC, RHnet
- No security team in operation: 8
ISTF, JSCC, LATNET, RESTENA, RoEduNet, SANET, ULAKBIM, University of Malta

Source: DJ2.3.1,1 /Sept 2006