

# I problemi di sicurezza nella rete dell'universita' e ricerca italiana GARR

Enzo Valente  
Direttore INFN-GARR

Security on the Net  
Parma, 11 Ottobre 2002

# "il GARR"



- L'acronimo **GARR** deriva da "Gruppo per l'Armonizzazione delle Reti della Ricerca".
- Questo Gruppo si e' autocostituito nel 1987 allo scopo di rappresentare organicamente la comunita' scientifica delle Universita' e degli Enti Pubblici di Ricerca italiani nelle attivita' di realizzazione, gestione, ricerca e utilizzazione delle reti informatiche nei confronti della Commissione Europea e nei confronti delle organizzazioni di Reti di Ricerca gia' esistenti nei paesi culturalmente ed economicamente piu' avanzati.
- Il **GARR** si costituisce formalmente nel 1989 come organismo del **MURST** (ministro Ruberti). Il MURST nomina la **CRCS** (Commissione per le Reti e il Calcolo Scientifico) e l'**OTS-GARR** (Organismo Tecnico-Scientifico)

## “la Rete GARR”

- **GARR** e' anche il nome assegnato alla Rete informatica dell' Universita' e della Ricerca Scientifica italiana.
- La Rete GARR interconnette tutte le Universita' (Statali e non) e tutte le sedi degli enti di ricerca scientifica (CNR, ENEA, INFN, Osservatori, etc.), nonche' istituzioni culturali o di ricerca a carattere accademico, scientifico e tecnologico per un totale di circa 270 siti.
- La Rete GARR e' interconnessa a tutte le Reti della Ricerca mondiali e, separatamente, al Global Internet.

# La Storia della Rete GARR

- Armonizzazione e sinergia tra Università' e Enti di Ricerca
- **1973-1990**: reti indipendenti di CNR, ENEA, INFN e Università'.
- **1990-1994**: rete **GARR**, prima rete unitaria di Università' e Ricerca
- **1994-1998**: rete **GARR-2** (evoluzione di GARR-1)
- **1998-2002**: rete **GARR-B** (Broadband)
- **2002-2006**: rete **GARR-G** (Giganet)

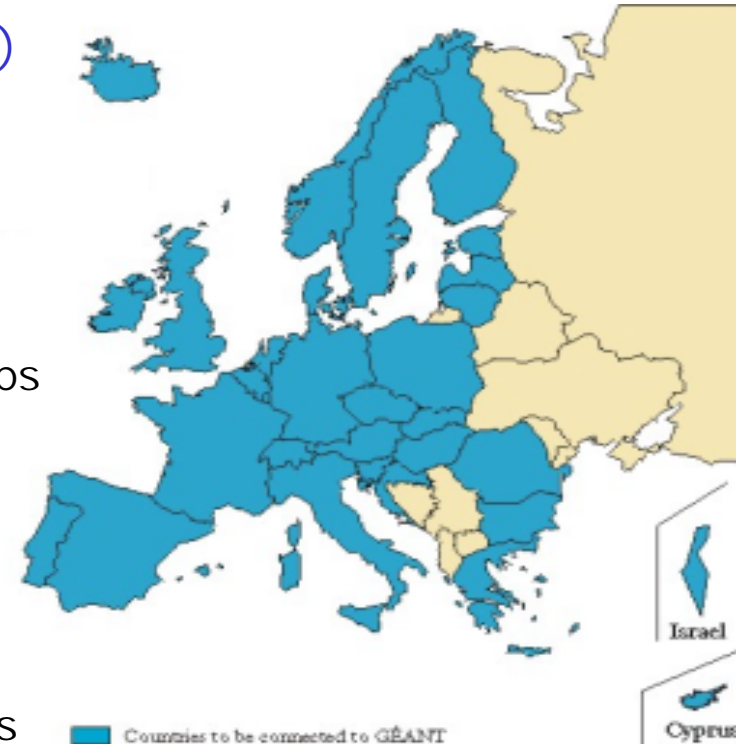
# GARR-B Fase 4 (Aprile 2002)



- Backbone nazionale
  - RM-NA-MI-BO@10Gbps
  - [2003: 40Gbps]
  - 18 MPoP, 4 GPoP
  - [2003: 20MPoP, 9 GPoP]
- Accessi Univ., CNR, ENEA, INFN, etc.
  - ~270 siti@2M-1Gbps
  - ~2.000.000 di utilizzatori (in Italia)
- Peering Ricerca Internazionale
  - Milano-GEANT@2\*2.5Gbps
  - R%D-Geant@10Gbps [VPN, QoS, etc.]
  - R%D-6Net@2\*155Mbps [Ipv6]
  - Catania-EU-MED-Connect
- Peering di Commodity
  - Roma-KQ[Telia]@622Mbps
  - Milano-GX@2.5Gbps
  - Roma-NAMEX@1Gbps
  - Milano-MIX@155Mbps [1Gbps nel 2003]

## La rete della Ricerca Europea GÉANT (1/2)

- Progetto **GÉANT** (evoluzione di TEN155)
- Cofinanziamento CE (5<sup>th</sup> FP) per 80M€ pari al 40% del costo di GÉANT
- Durata 48 mesi (1/12/00 – 30/11/04)
- Caratteristiche principali di GÉANT:
  - Backbone su lambda ridondate da 10Gbps
  - Uso di tecnologia DWDM
  - Peering con tutte le reti della ricerca mondiali
  - Supporto per QoS e VPN
  - Accesso reti ricerca nazionali fino a 10 Gbps per produzione e a ulteriori 10Gbps per sperimentazione.

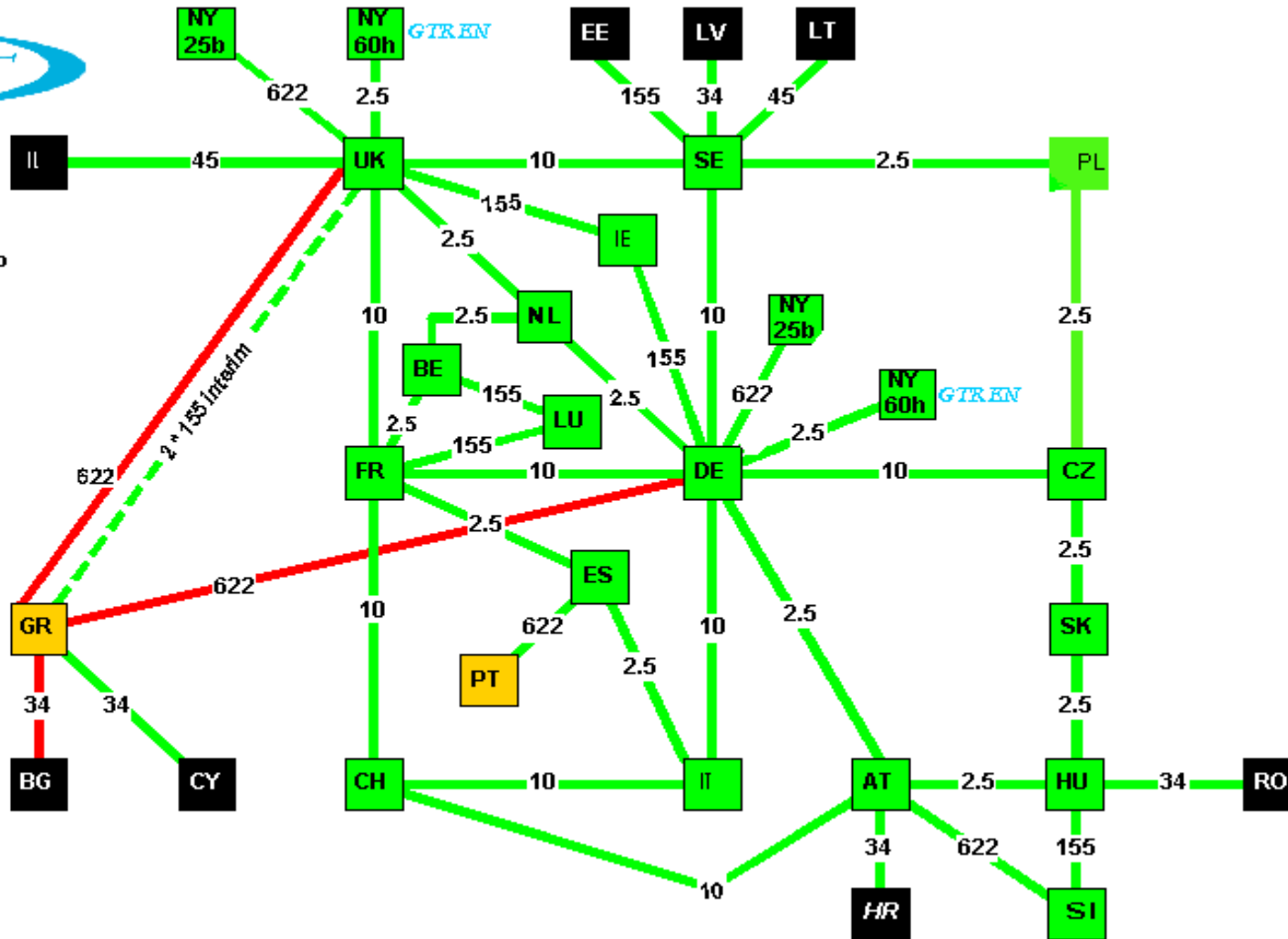




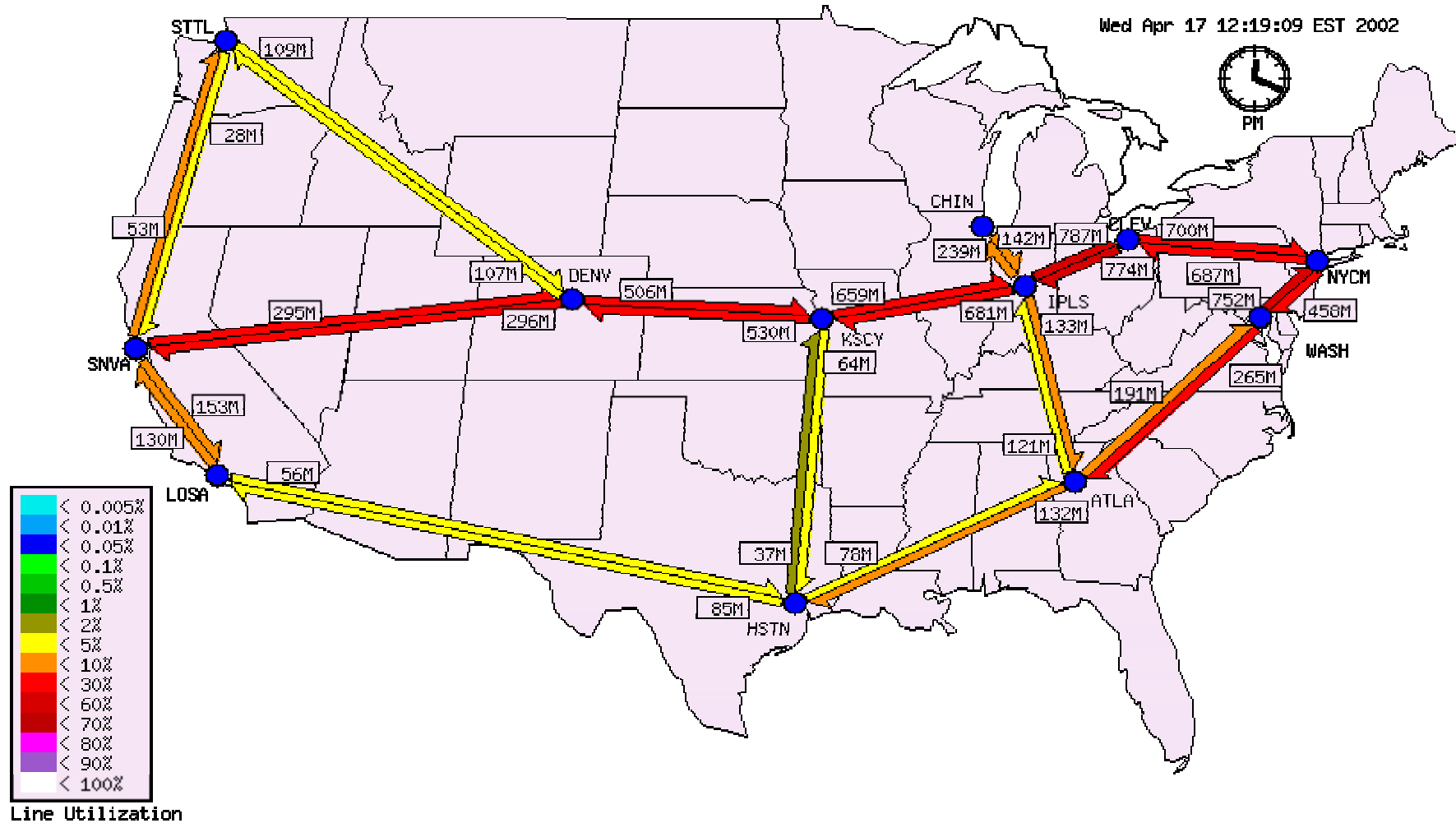
GEANT Topology  
6 February 2002  
ops-01-065w05

- XX No GEANT POP
- XX POP Pending
- XX POP delivered

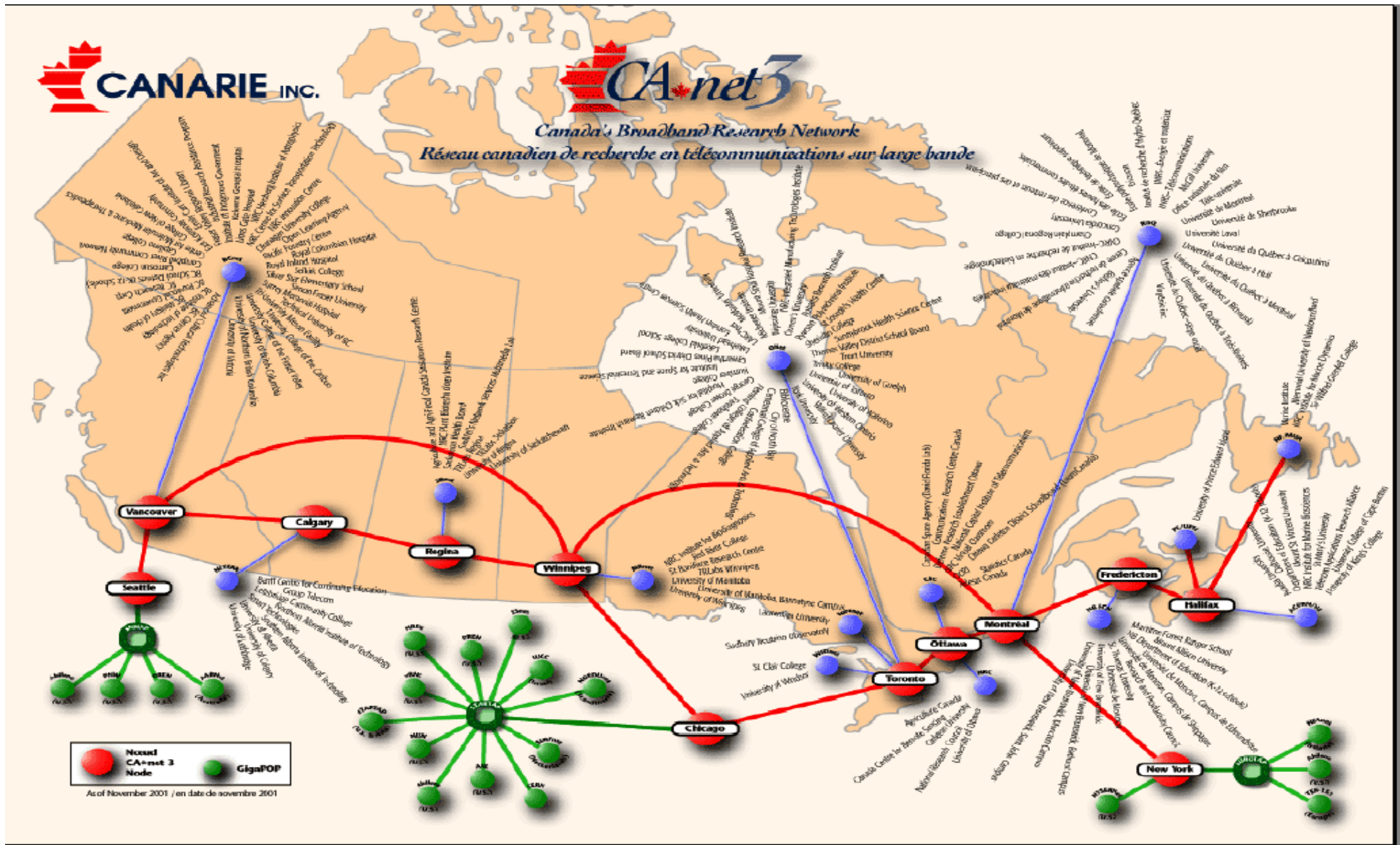
- pending
- delivered
- testing
- accepted



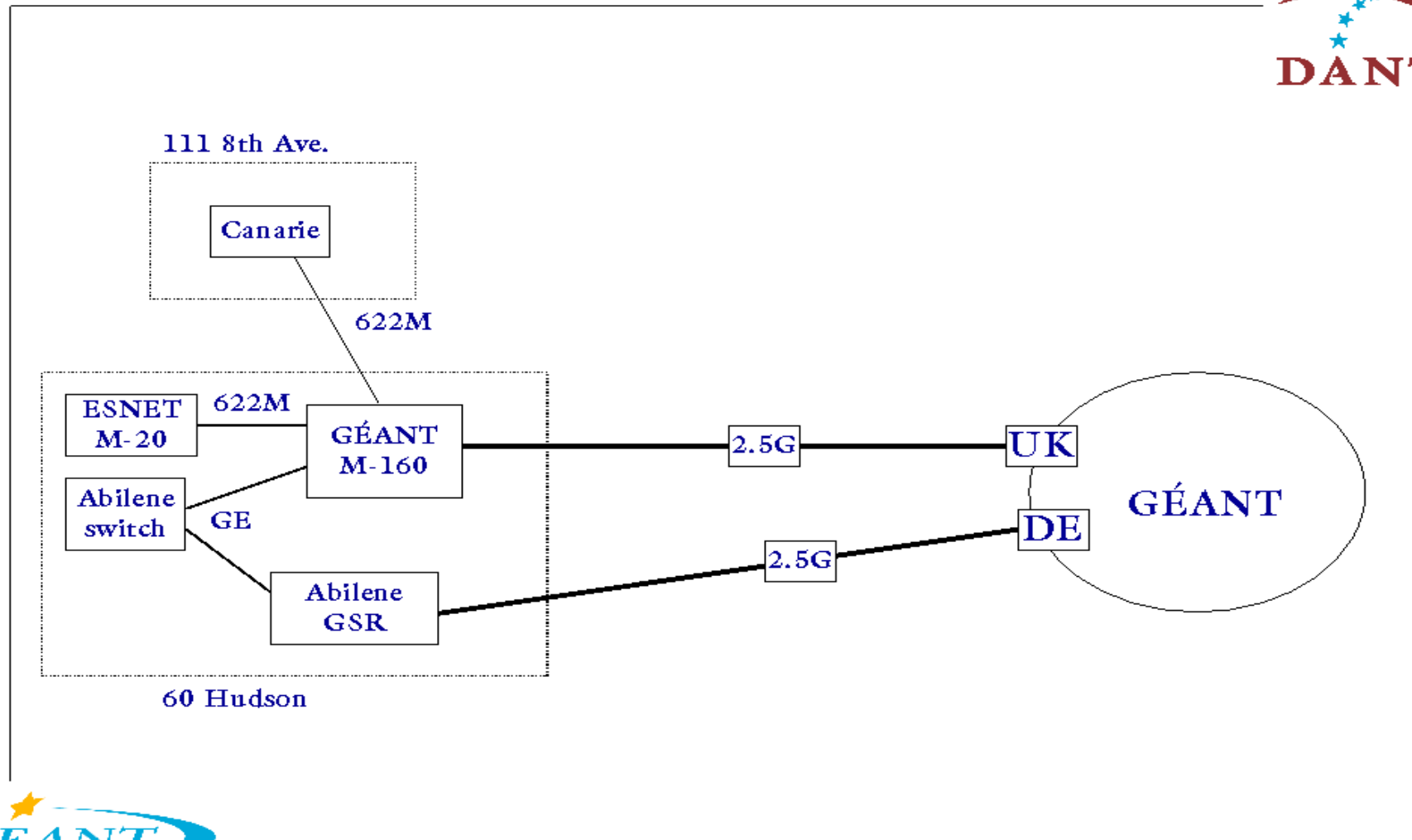
# La rete della Ricerca statunitense Abilene



# La rete della ricerca canadese Canarie



## • Transatlantic Peering (for Research only)



# Cosa offre la Rete GARR

- Accessi al backbone in ATM, V35, SDH e Ethernet fino a 1Gbit/sec
- IP "Best-Effort" per le applicazioni classiche:
  - *www, e-mail, telnet, ftp, news, etc.*
- Managed Bandwidth Service (MBS) :
  - costruzione di reti virtuali private (VPN):
  - interconnessione tra gli appartenenti di una stessa collaborazione scientifica nazionale o internazionale.
  - gruppi di lavoro all'interno di un esperimento (ad es. *sviluppo di software cooperativo*)
- Quality of Service (QoS)
  - Applicazioni a banda garantita
  - Sperimentazione nuove tecnologie e applicazioni
  - IP Premium
  - Multicast

# Gestione Rete GARR

- La Direzione GARR cura:
  - la pianificazione, l'evoluzione, il coordinamento tecnico e il funzionamento della rete (gruppo GARR-TEC, [tec@garr.it](mailto:tec@garr.it)) in accordo con i rappresentanti (APM e APA) dei siti connessi alla rete
  - il coordinamento della sperimentazione di nuove tecnologie della rete GARR e la partecipazione nei comitati e nei progetti internazionali
  - la gestione amministrativa e scientifica ([garr-b@garr.it](mailto:garr-b@garr.it))
- Servizi di network del GARR sono:
  - GARR-NOC (call centre, [noc@garr.it](mailto:noc@garr.it))
  - GARR-LIR (assegnazione indirizzi e reti IP, [lir@garr.it](mailto:lir@garr.it))
  - GARR-NIC (domini di II livello SOLO per GARR, [nic@garr.it](mailto:nic@garr.it))
  - GARR-CERT (CSIRT, security, [cert@garr.it](mailto:cert@garr.it)) [INFN- Firenze]
  - GARR-MCAST (multicast, [mcast@garr.it](mailto:mcast@garr.it))
  - Web-Cache, FTP-Mirror ([cache@garr.it](mailto:cache@garr.it), [mirror@garr.it](mailto:mirror@garr.it)) [CILEA]
  - Usenet News ([news@garr.it](mailto:news@garr.it)) [SerRA, Universita' di Pisa]

## Il problema delle sicurezze nella rete GARR

- Priorita' nella rete GARR:
  - banda passante capace di assorbire picchi di uso a livello nazionale e internazionale;
  - ridondanza e affidabilita' dei collegamenti;
  - Managed Bandwidth Service (modularita', QoS, VPN);
  - adeguamento continuo alle reti piu' evolute;
  - **sicurezza dati e sistemi**

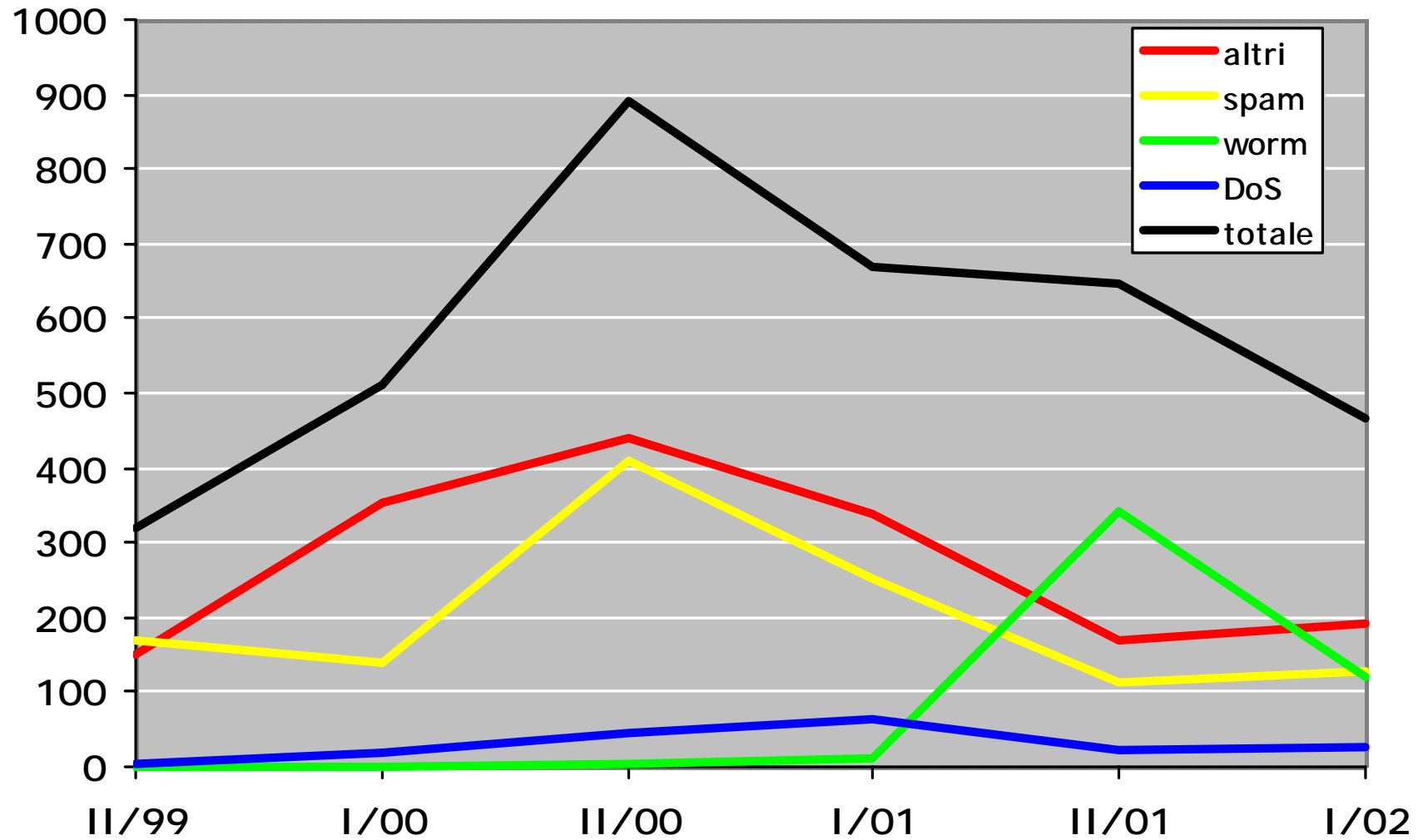
## Lo CSIRT del GARR-CERT

- Lo CSIRT della rete GARR:
  - in attività dal Giugno 1999;
  - opera in stretta collaborazione con il Network Operation Center (GARR-NOC).
- Risorse umane:
  - nucleo operativo (sede a Firenze): 3 (2 full-time);
  - esperti e “ufficiali di collegamento”: 5;
  - contatti locali (APM):  $\approx$  280.
- “Trusted Introducer” Level 2 Team  
(<http://www.ti.terena.nl/>)

## le compromissioni sui sistemi e sulla rete

- Scansioni;
- attacchi
- virus;
- Riproduzione (worm);
- Bot IRC;
- Warez;
  
- Attacchi (D)DoS alla rete (*smurf, trinoo, tfn, tfn2k, stacheldraht, ...*);
- Attacchi ad altri nodi (in special modo sulla stessa LAN);
- Sniffer;

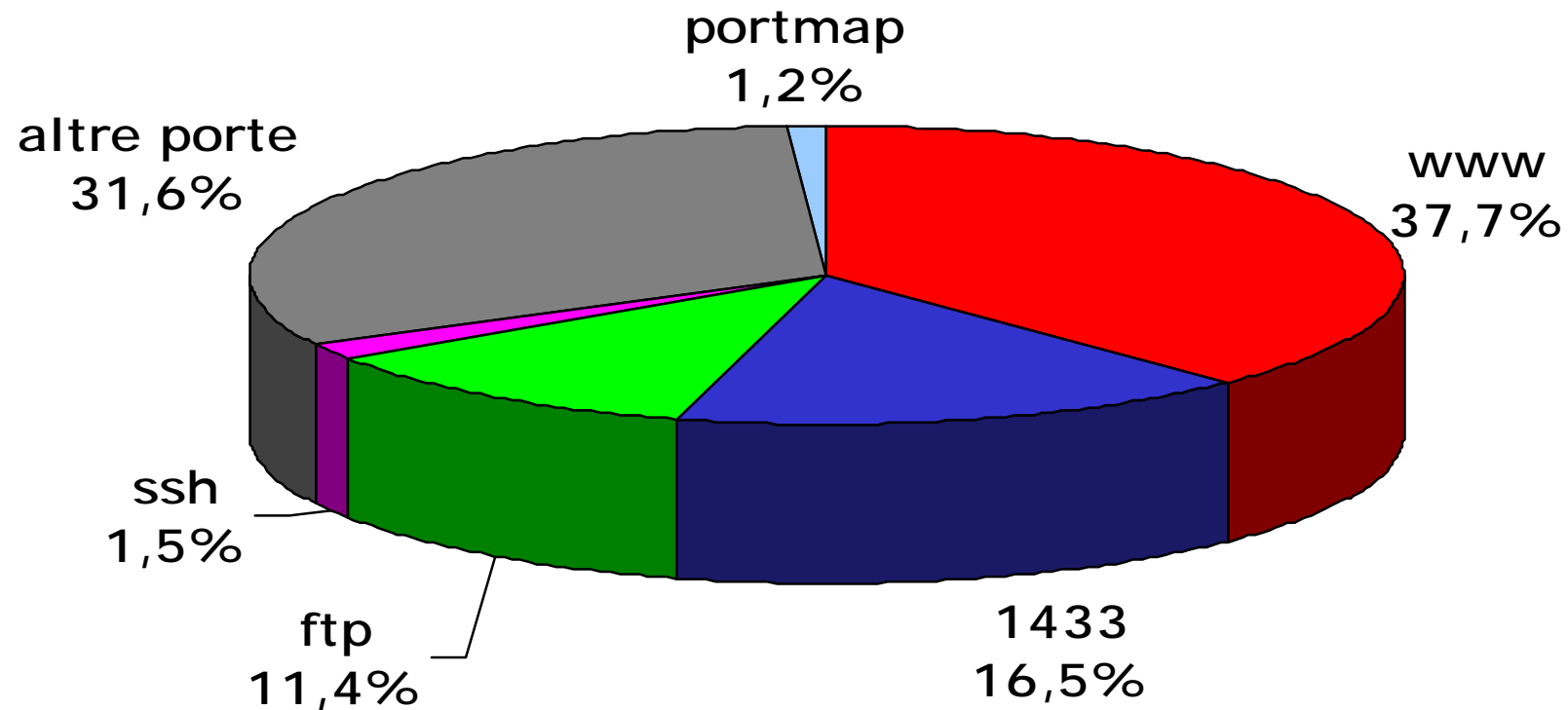
# Incidenti segnalati a GARR-CERT



# Honeypot

- Esperimento al San Diego Supercomputer Center (SDSC):
  - **23/12/99**: installazione completa di RedHat 5.2 su di una macchina inutilizzata e tenuta sotto osservazione;
  - **14/1/00**: probe per Solaris RPC;
  - **14-18/1/00**: prova di 20 exploits (POP, IMAP, telnet, RPC, mountd ...) falliti perchè per RedHat 6;
  - **xx/2/00**: compromissione via vulnerabilità POP e installazione di rootkit e sniffer;
  - **18/2/00**: altra compromissione, server web defacing, diffusione notizia su IRC e segnalazione di attrition.org.
- Lo stesso esperimento ripetuto nel 2001:
  - prima scansione dopo **30 secondi**;
  - primo tentativo di compromissione dopo **1 ora**;
  - compromissione completa dopo **12 ore**.

## Scansioni nel periodo 10-17/6/02



da <http://www.incidents.org/>

# Modus operandi

## ⊗ Attacco:

### – da remoto:

- utilizzo di un exploit su un servizio (ad es. ftp) con ottenimento shell di root;

### – da locale:

- login con password “legittima”;
- scarico via rete programma di exploit;
- compilazione, esecuzione e ottenimento shell di root.

## ⊗ Installazione *rootkit* (e altre *backdoor*).

## ⊗ Cancellazione tracce.

## ⊗ ...

## Vulnerabilità più gravi (tutti i SO)

Da <http://www.sans.org/>:

- Installazioni *non personalizzate* di sistemi operativi e applicazioni.
- Account senza password (o con password banali).
- Backup inesistenti o incompleti.
- Servizi attivi non necessari.
- Mancanza di controllo sugli indirizzi dei pacchetti.
- Logging inesistente o incompleto.
- Programmi CGI vulnerabili.

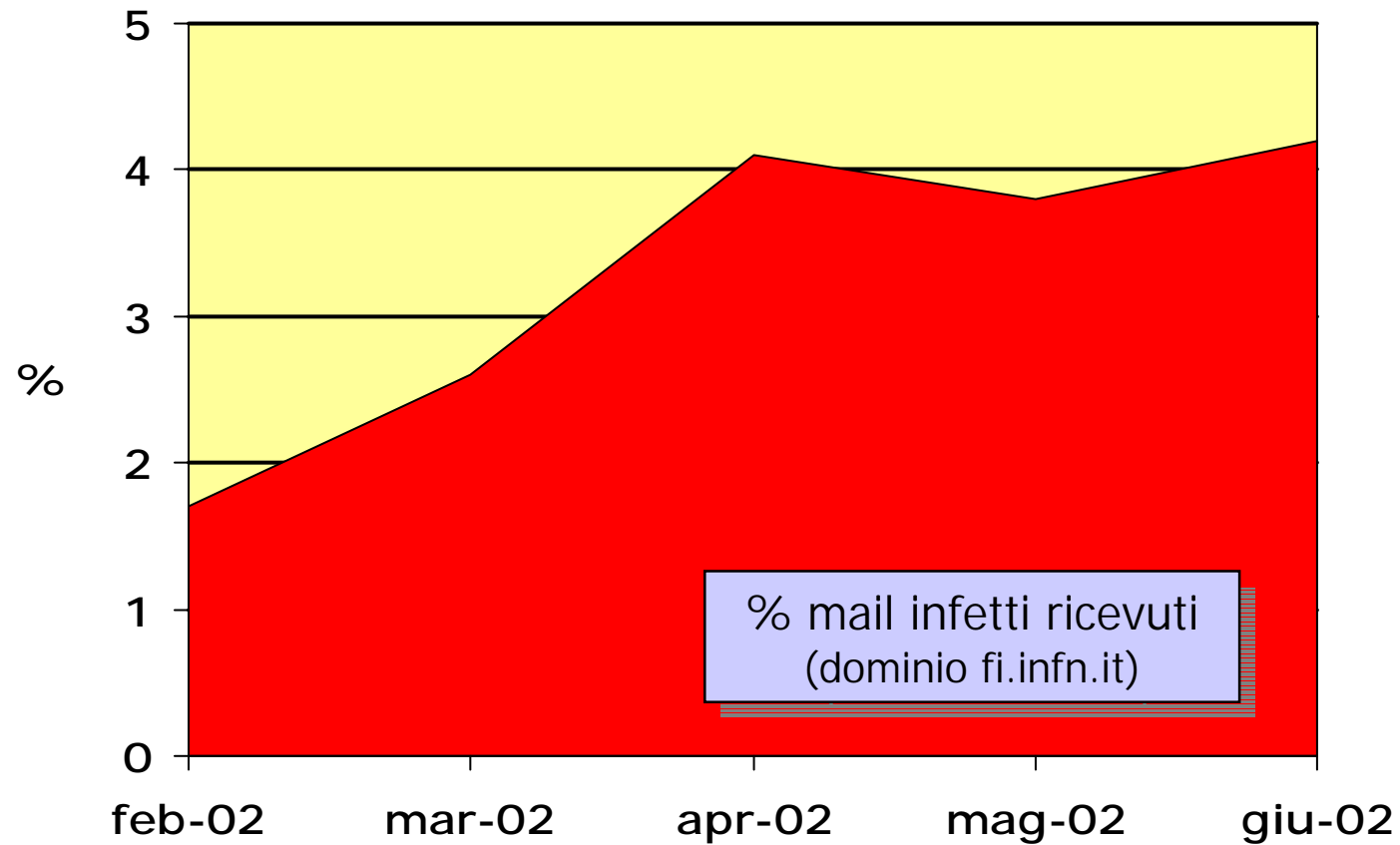
## Vulnerabilità più gravi (Unix)

- wu-ftpd (*File Globbing Heap Corruption*).
- sendmail (open mail relay).
- lpd (remote print protocol daemon).
- sadmind e mountd.
- SSH (*CRC32 Compensation Detection Attack*).
- servizi rpc.
- bind.
- SNMP.
- Common Desktop Environment (*CDE dtspcd Buffer Overflow*).

## Vulnerabilità più gravi (Windows)

- Unicode Vulnerability (Directory Traversal Attack) (**Nimda**).
  - NT 4.0 con IIS 4.0 e 2000 server con IIS 5.0, senza SP2
- ISAPI Extension Buffer Overflow (**Code Red**).
  - NT4, 2000 Server, Advanced Server e Server Data Center Edition con IIS 5.0, senza SP2.
- IIS Remote Data Services.
  - NT4 con IIS e directory virtuale \msadc.
- NETBIOS: esposizione di risorse non protette.
  - L'attaccante può ricavare informazioni utili per attacchi successivi: username, chiavi del Registry, ecc.

# Virus via mail



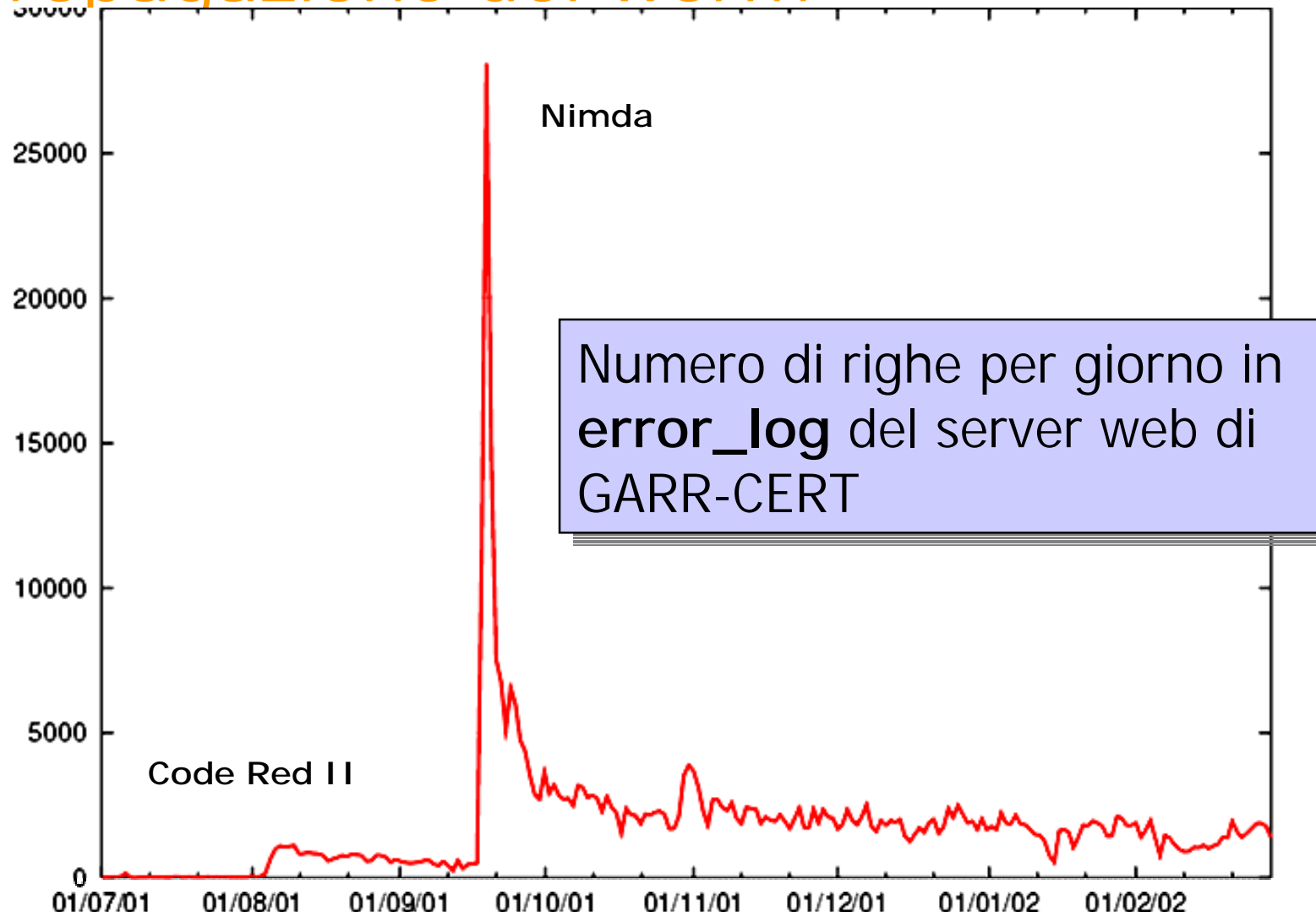
## I worm 1/2

- Un worm è del codice ostile in grado di autopropagarsi da solo, senza necessità di intervento dell'utente (a differenza dei virus).
- La combinazione di un meccanismo di propagazione veloce con una grande diffusione della vulnerabilità sfruttata produce velocità di propagazione impressionanti.
- Spesso l'effetto più importante è il denial of service provocato dalle scansioni alla ricerca di nuovi sistemi da compromettere.

## I worm 2/2

- Social Engineering
  - W32/Sircam.
- Specifiche vulnerabilità
  - sadmind/IIS worm;
  - Code Red, Code Red II;
  - Nimda;
  - Spida/SQLsnake/Digispid.
- Le principali vittime sono utenti windows:
  - meno sofisticati tecnicamente,
  - meno protetti,
  - meno attenti ai security alert.

# Propagazione dei worm



Numero di righe per giorno in **error\_log** del server web di GARR-CERT

# Attacchi Dos

- Tipi
  - TCP floods
  - ICMP echo request/reply (ping floods)
  - UDP floods
- Il mittente è sempre falsificato: **fondamentale** che **tutti** i router siano configurati per controllare la legittimità degli indirizzi dei pacchetti in entrata e in uscita.

# Attacchi DDos

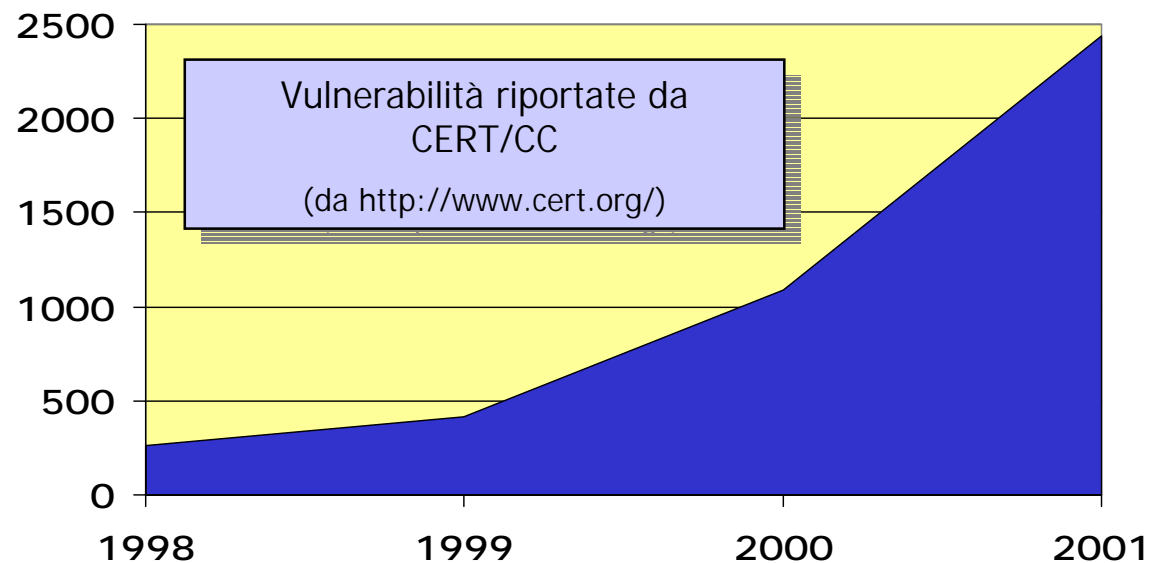
- Centinaia di “agenti” (compromessi da tool automatici) comandati via icmp o irc:
  - l'intruso invia il comando *all'handler*;
  - l'*handler* comunica il bersaglio e il tipo di attacco agli agenti;
  - gli agenti attaccano il bersaglio prescelto.
- Sono stati registrati flussi dell'ordine dei Gbps.

# Servizi da bloccare o controllare

- Da raccomandazioni di CERT/CC
  - Login: 21/T, 22/T, 23/T, 139/T, 512-514/T
  - RPC & NFS: 111/TU, 2049/TU, 4045/TU
  - NetBIOS: 135/TU, 137-138/U, 445/TU
  - X Windows: 6000-6255/T
  - Naming: 53/TU, 389/TU
  - Mail: 25/T, 109-110/T, 143/T
  - Web: 80/T, 443/T
  - Small Services: <20/TU, 37/TU
  - Vari: 69/U, 79/T, 119/T, 123/T, 161-162/TU, 179/T, 514/U, 515/T, 1080/T
  - ICMP: ...
- **Molto meglio bloccare tutto e aprire caso per caso!**

## Il futuro 1/2

- La qualità del software prodotto non sembra migliori:
  - la durata del ciclo sviluppo-prova-rilascio software è in continua diminuzione;
  - continua a essere rilasciato software con vulnerabilità di tipo ormai ben noto (ad es. *buffer overflow*).



## Il futuro 2/2

- Prevedibile una nuova generazione di worm e virus più virulenti.
- I nodi GARR, con l'aumento della banda a disposizione, sono molto appetibili come strumenti per attacchi (D)DoS.
- Nuove tecnologie pongono nuovi problemi di sicurezza
  - “griglie” di calcolo (ad es. DataGRID);
  - nuovi protocolli “firewall-friendly”;
  - P2P;
  - wireless;
  - ...

# Case Study: la sicurezza applicata alle Computing Grid



- Problemi particolarmente complessi oggi richiedono sofisticate infrastrutture di calcolo (software e hardware)
- Per i futuri esperimenti di HEP la potenza di calcolo necessaria non sara' piu' "confinabile" in un singolo sito
  - potenza di calcolo (K-SI95 ~7.500 → ~200.000 PIII 800MHz !!! )
  - ~PetaByte di dati
- I modelli di calcolo distribuito oggi esistenti non sono sufficienti a risolvere il problema:
  - clusters → *fabrics*
  - produzioni/analisi locali → *produzioni/analisi distribuite*
  - collaborazioni internazionali sempre piu' grandi

➔ Grid

# Che cos'è la "Grid Technology"?

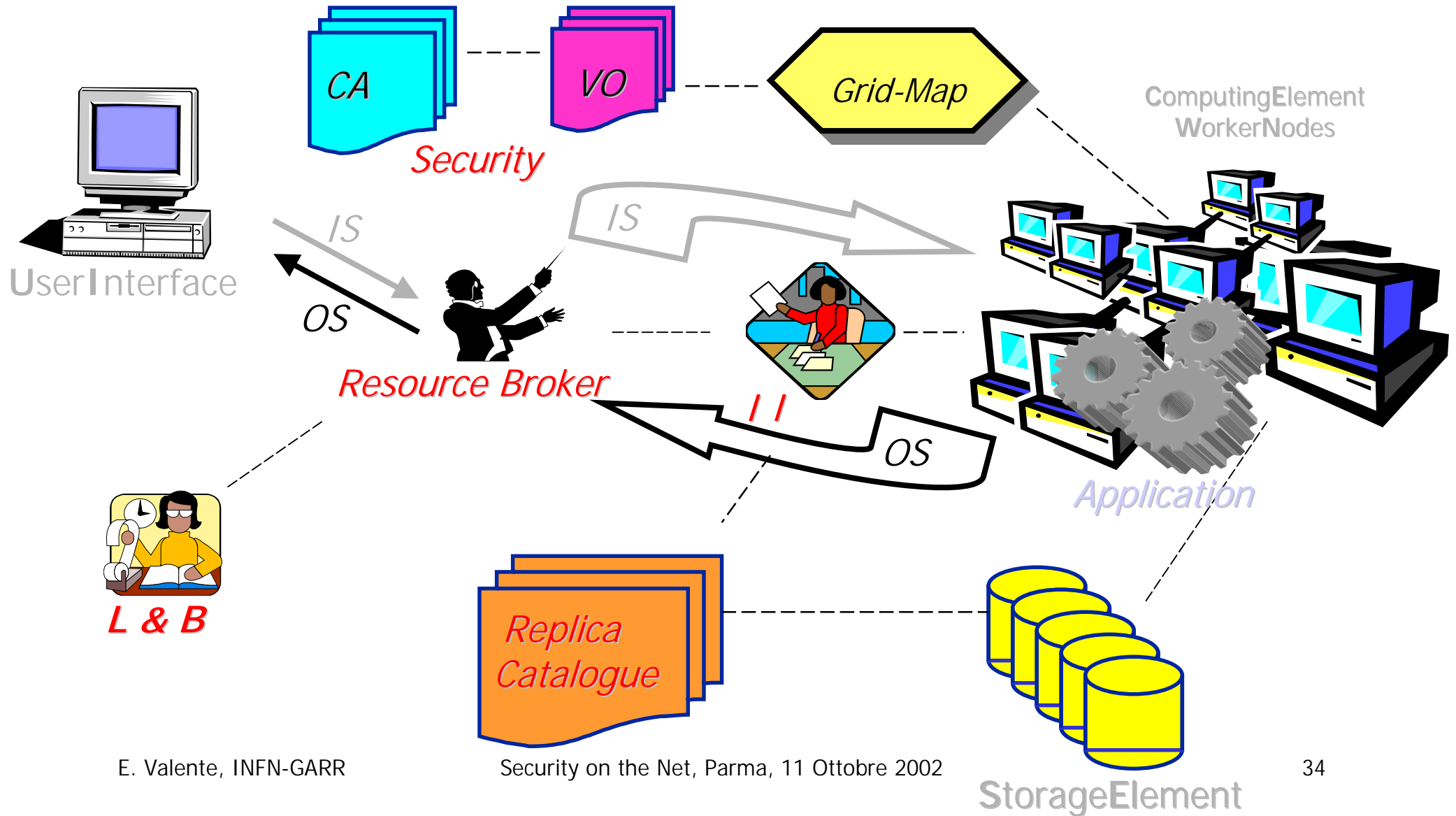
- L'obiettivo principale dei progetti di Grid è lo sviluppo di un insieme coerente di risorse di calcolo ("Grid"), distribuite su scala geografica.
- La Grid dovrà garantire la gestione di data-sets di differenti "Virtual Organizations" (fino alla scala del "Peta-Byte") utilizzando computing power e storage distribuiti.
- Una Griglia Computazionale dovrà fornire una interfaccia uniforme ai suoi utilizzatori (ed alle sue risorse), distribuendo un servizio affidabile e accessibile da "qualsiasi luogo"
- Una griglia, in breve, è quel "*bit*" di cui non vogliamo preoccuparci, purché esista, in analogia con le griglie-elettriche (si inserisce un "dispositivo" nella presa nel muro e si opera senza preoccuparsi delle centrali elettriche di produzione, della rete di distribuzione, del trasporto su cavi ad alta tensione, etc.)

# Problemi di sicurezza "preventive" nelle Virtual Organization

- La tripla A: Authentication, Authorization, Accounting
- Authentication (X509-PKI, PGP, coordinamento CA)
- Authorization (LDAP per ogni VO, meccanismo tipo DHCP dinamico)
- Accounting (standard...)

➔ Grid

# Tipico "Grid-job life-cycle"



## Attività preventive

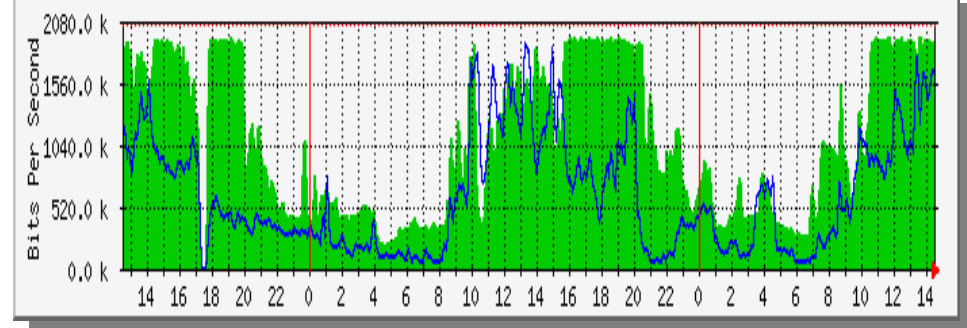
- Incontri tecnici periodici tra i responsabili delle sicurezze (formazione);
- Scansioni alla ricerca di vulnerabilità (nel 2001 il GARR-CERT ne ha operate circa 60);
- Verifiche periodiche sullo stato dei nodi già coinvolti in incidenti;
- SENTINEL: Sistema di allarme per attacchi DoS in corso (in collaborazione con GARR-NOC);
- Segnalazione di Alert.

## Attività preventive: SENTINEL

- Sistema di allarme via e-mail (GARR-NOC):
  - attacchi (D)Dos;
  - server warez;
  - p2p mal configurati;
  - ecc., ecc..

```
From: noc@garr.it  
To: sentinel@fi.infn.it  
Cc: noc@garr.it  
Subject: SENTINEL notification  
N. 3 for: NA-CNR_Napoli_Link_2
```

```
WARNING: Abnormal Traffic for  
NA-CNR_Napoli_Link_2 on Wed Jun  
26 13:30:00 2002
```



## Gli "Alert"

- Vulnerabilita' del software commerciale
- Segnalazioni dei principali alert pubblicati (virus, worm, etc.).
- Pubblicazione di note d'uso, esperienze, tutorial, how-to, ecc.
  - i contributi degli utilizzatori della rete sono indispensabili
    - vengono spediti a [cert-staff@garr.it](mailto:cert-staff@garr.it);
    - verranno valutati da un mini comitato editoriale e, se ritenuti di interesse generale, inviati a [security@garr.it](mailto:security@garr.it) e pubblicate sul server web di GARR-CERT.



## eCSIRT: obiettivi

- Progetto europeo.
- Obiettivi:
  - definizione di un linguaggio comune per lo scambio di dati tra CSIRT;
  - scambio di informazioni su incidenti, come normale prassi operativa tra CSIRT;
  - meccanismo di raccolta di statistiche *non ambigue* di incidenti;
  - raccolta di dati relativi ad incidenti al fine di fornire agli CSIRT informazioni di “early warning” da distribuire all’utenza.



## eCSIRT

- Durata 15 mesi.
- Partecipanti
  - M&I/Stelvio b.v. (NL)
  - PRESECURE Consulting GmbH (D)
  - GARR-CERT (I)
  - Le CERT Renater (F)
  - JANET-CERT (UK)
  - DFN-CERT GmbH (D)
  - CERT-Polska (PL)
  - DK-CERT (DK)
  - IRIS-CERT (E)



## Che fare? 1/2

- Stabilire (e far rispettare!) serie politiche di sicurezza a livello di Ateneo e Istituti di ricerca (compresa la creazione di nuovi CSIRT).
  - Direttiva della Presidenza del Consiglio dei Ministri (Dipartimento per l'Innovazione e le Tecnologie), *Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni* (16 Gennaio 2002):
    - autodiagnosi del livello di adeguatezza della sicurezza informatica e delle telecomunicazioni (ICT);
    - attivazione delle necessarie iniziative per posizionarsi sulla "base minima di sicurezza", che consenta di costruire con un approccio unitario e condiviso, le fondamenta della sicurezza della pubblica amministrazione;
    - promuovere la creazione e la successiva attivazione di un modello organizzativo nazionale di sicurezza ICT che comprenda tutti gli organi istituzionali, scientifici ed accademici deputati, ciascuno per il proprio ruolo, ad assicurare organicità e completezza al tema sicurezza.

## Che fare? 2/2

- Aumentare la consapevolezza degli utilizzatori sulla necessita' di configurare correttamente e di aggiornare tempestivamente il software del proprio sistema di calcolo.
- Mantenere aggiornati i dispositivi hardware e software di protezione dei sistemi di calcolo e delle reti locali, metropolitane e geografiche.
- Aumentare (in quantità e qualità) le interazioni tra gli CSIRT (in particolare con quelli degli ISP)
  - eEurope ActionPlan: *"Stimulating public/private cooperation on dependability of information infrastructures (including the development of early warning systems) and improving cooperation amongst national computer emergency response teams"*.



fine

