

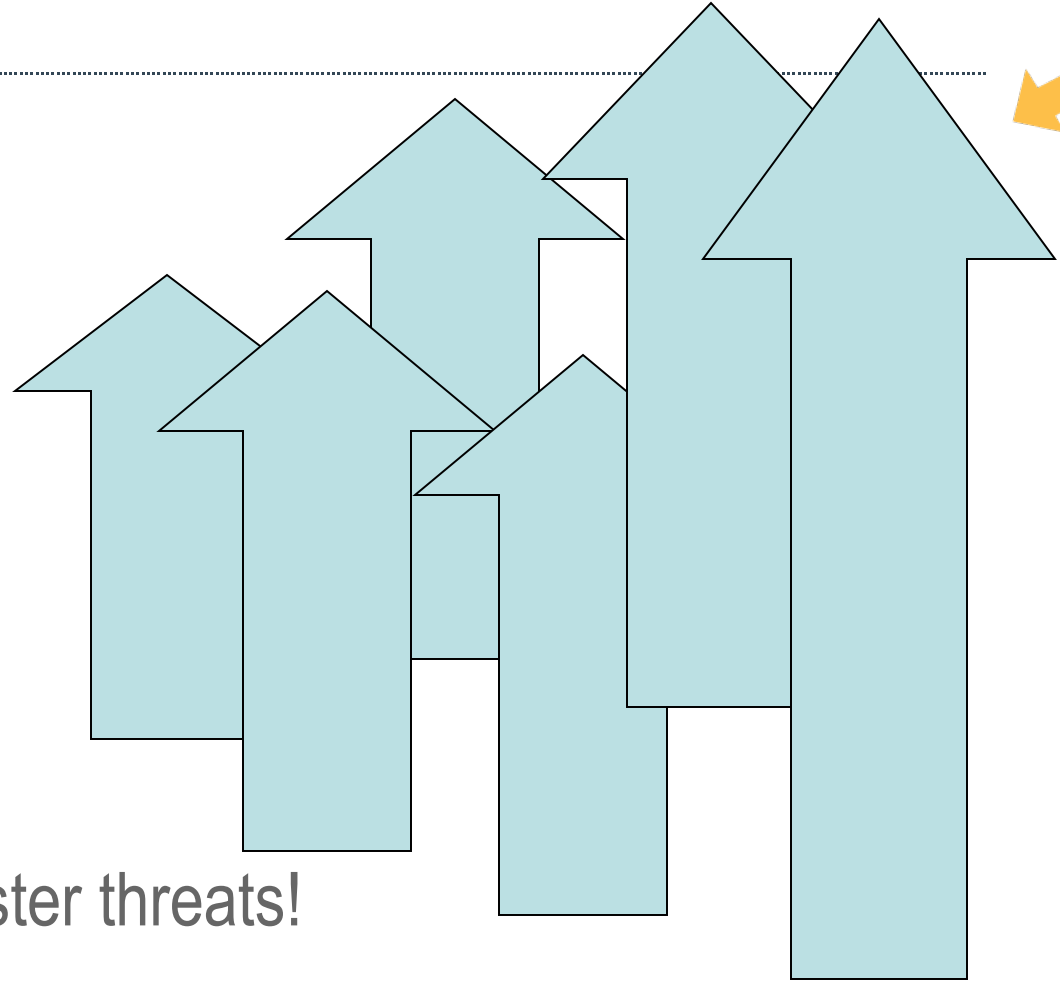
IGF Hyderabad 2008
Dimensions of Cyber Security
& Cyber Crime



Michael Lewis, Carnegie Mellon University
& Deputy Director, Q-CERT

General Trends

- ▶ Users on Internet
- ▶ Computers
- ▶ Devices
- ▶ Vulnerabilities
- ▶ Exploits
- ▶ Financial Incentives
- ▶ Criminal Activity
- ▶ & a multitude of sinister threats!



The Economics of CyberCrime



- ▶ Barriers to entry are minimal
 - resources are essentially free (!)
 - technical requirements are modest
- ▶ Low risk, high reward!
 - Opportunities grow with continued E-volution of services
 - Returns are tantalizingly large
- ▶ Prosecution is difficult
 - Investigation is costly in time & resources
 - Challenging to trace and attribute
 - Coordination of investigations across borders is difficult
 - And what is a crime in some countries is not in others
- ▶ And innovation seems to be prevalent on the “dark” side – consider botnets!
- ▶ **Cybercrime is a growth industry!**

Agreed – the Internet is good but it was not designed for “security”



- ▶ What do we mean by “security”? Integrity? Privacy? Safety?
 - The parable of the three blind men and the elephant
- ▶ Better to be proactive than reactive ... but “we live in interesting times” ... prepare for the worst ... incidents happen!
 - Assume loss of a USB ... or that clear text is essentially public
- ▶ Everyone is already doing something ... do it better! In accordance with the growing body of experience & best practices
- ▶ Use relevant and useful standards and policies
 - adapt approach to national / local situation
- ▶ Many have come before ... utilize their experience, insights, recommendations ... complement, not conflict ... mutually reinforce
 - contribute to the **Cyber Security Network!**

When Things Go Wrong, Who Do You Call?



- ▶ Do people know what to do in a crisis?
 - Would they recognize it when it happens?
 - Are escalation thresholds and procedures established?
 - When should (or not) law enforcement get involved?
- ▶ Are roles defined?
 - Issues of authority, responsibility, & liability
- ▶ Do trusted relations exist?
 - Must be established in advance of actual need!
- ▶ Such questions should be asked at all levels
 - Individual
 - Organizational
 - national

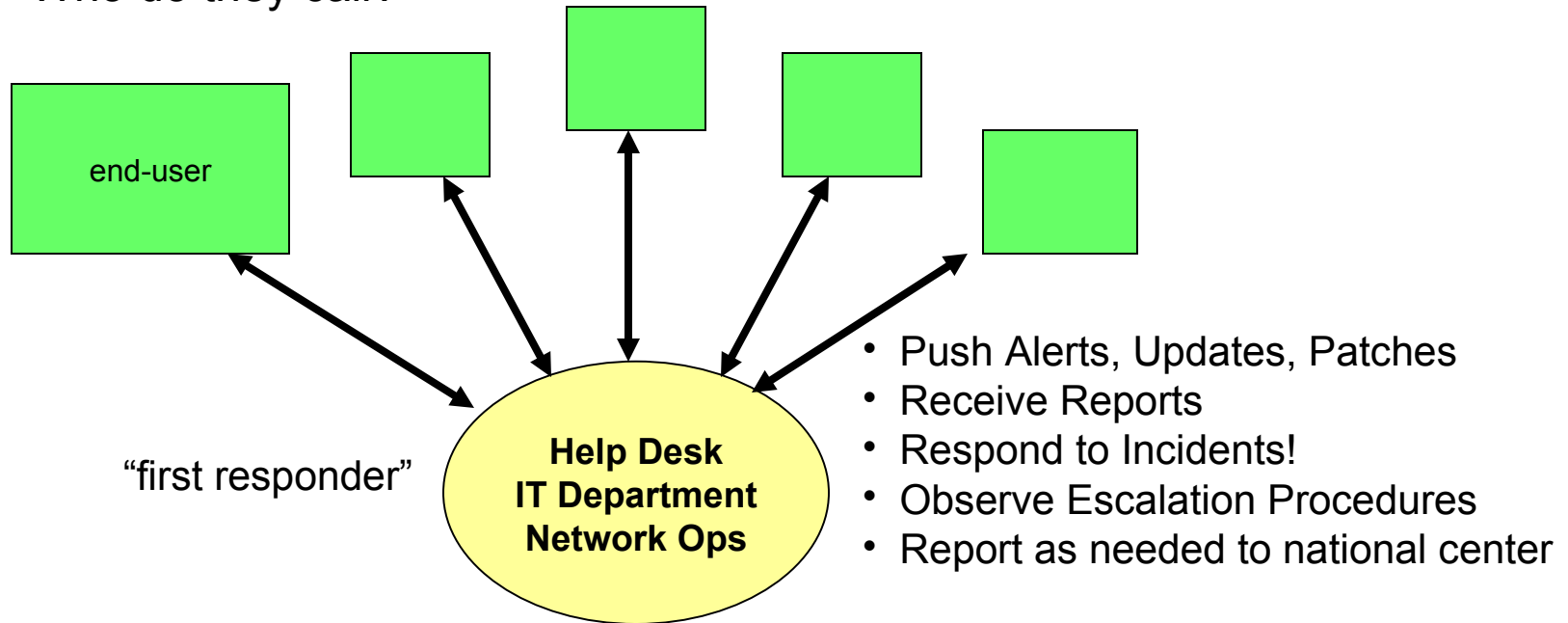
One Component of Improved Cyber Security



- ▶ A “Computer Security Incident Response Team”
- ▶ Can exist within an organization, a sector, or at a national, regional, or sector level
- ▶ Should be proactive more than reactive
- ▶ Also known as a “CERT” – a Computer Emergency Response Team
- ▶ The original is the CERT/CC at the Software Engineering Institute of Carnegie Mellon University

“Front-Line” Response

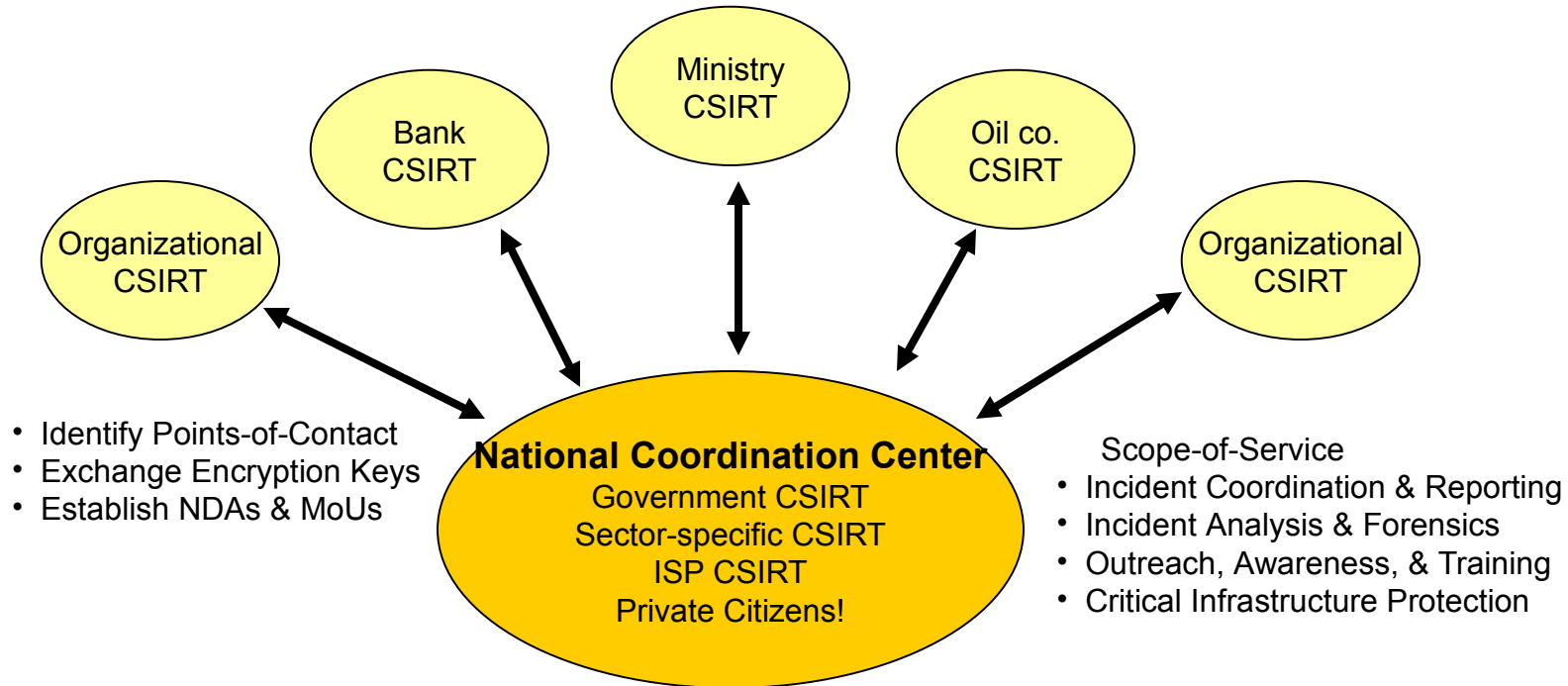
Who do they call?



An organizational CSIRT
to formalize organizational incident response

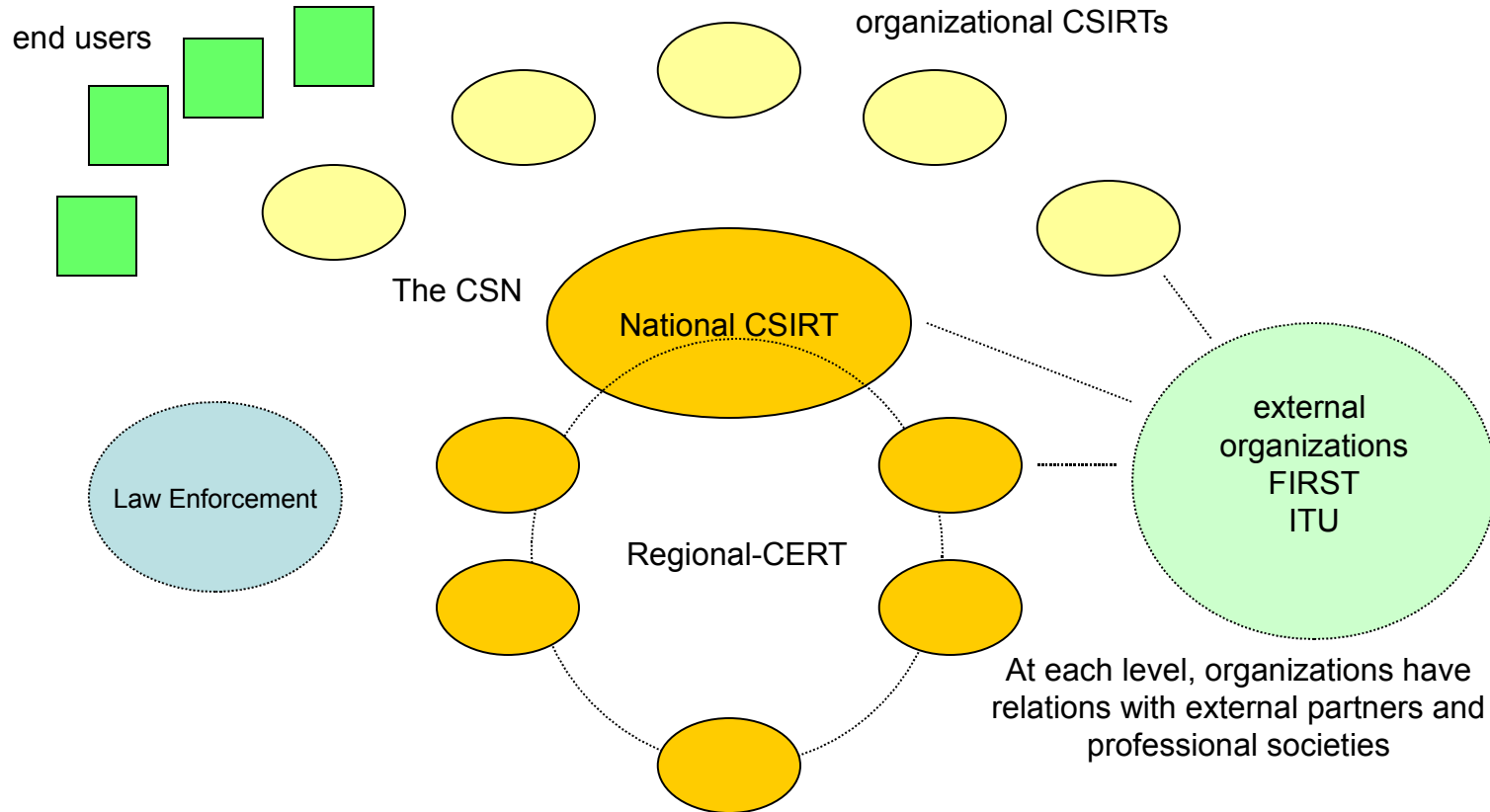
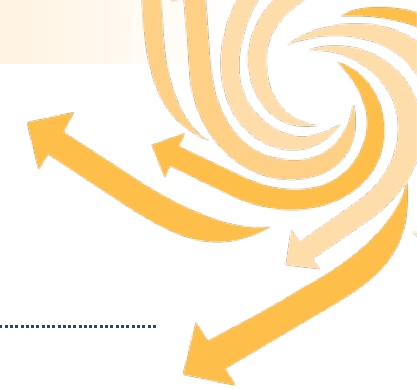
National CSIRT

a necessary but not sufficient component
of a national cyber security strategy



The National Cyber-Security Network

The Cyber Security Network

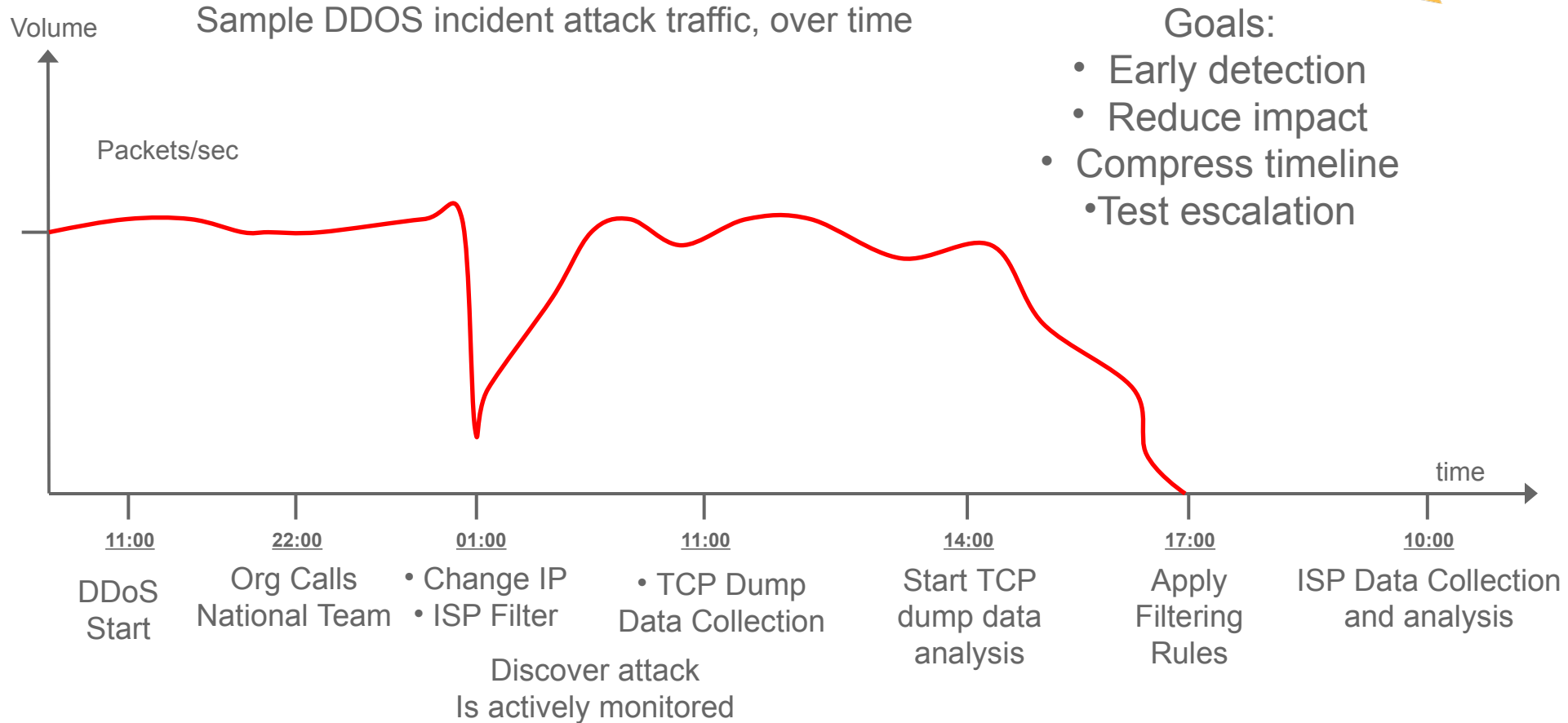


Coordinating a National Approach to Cybersecurity



- ▶ Develop a National Cybersecurity Strategy – identify and engage the stakeholders
- ▶ Create Incident Management & Coordination Capability – consider the CSIRT model
- ▶ Identify constituents & counterparts – national, regional, international
- ▶ Establish trusted relations & secure mechanisms for collaboration
- ▶ Conduct regular, targeted events to build skills, test systems and escalation procedures, & share experience

Review Incidents & Improve Response



Aftermath Questions



- ▶ What can be done to improve detection and response?
- ▶ When did the attack actually start? When did it stop?
Was there a discernible pattern that might help future early detection strategies?
- ▶ Review the impact of mitigation strategies – what worked?
What didn't?
- ▶ Review the sequence of deploying the mitigation strategies – was order important?
- ▶ Was the proper escalation procedure observed?
- ▶ Were the right partners involved?

General Questions



- ▶ Are first-responders identified and properly trained?
- ▶ Are there “default” strategies that can be designed in advance and rapidly deployed for different types of incidents?
- ▶ If so, what is the threshold / trigger for their activation?
- ▶ Are escalation procedures defined? Are forensically-safe mitigation and analysis methods used?
- ▶ What are the respective roles and responsibilities of targeted site / ISP / CSIRT?
- ▶ Are there liability issues involved, regarding intervention and advice?

Such questions should be resolved by the cool light of day rather than in the heat of the moment when time is of the essence!

Align & Partner

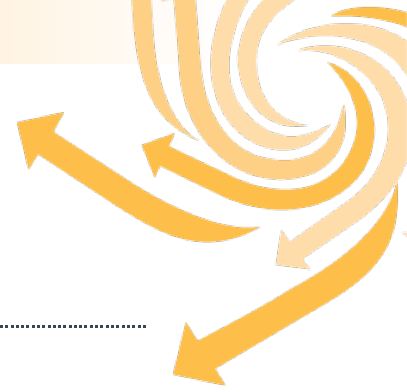
many good initiatives exist



Microsoft



Provocations



- ▶ How much security do we need / want?
- ▶ What kind of security (transactional, privacy, safety)?
- ▶ How are controls implemented without damaging the nature of the Internet?
- ▶ How much anonymity (if any!) ?
- ▶ Who holds data? Under what guidelines (duration, access, distribution)?
- ▶ Is the Internet as constituted suitable for children? If not, what should be done? Awareness? Tools?

Questions – at the end! & this afternoon

