Welcome to the World of Standards

ETSI

World Class Standards

Standardisation – the route to deployment

Scott CADZOW

Disclaimer

- My job is standards
- I am informally representing ETSI
- I am the rapporteur at ETSI of a work item in the Cyber-Security domain on assuring ICT security for CI

Definitions

- All activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability
- The analysis, warning, Information Sharing, vulnerability reduction, risk mitigation and recovery efforts for networked information systems

Definitions

- All activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability

CIP

- The analysis, warning, Information Sharing, vulnerability reduction, risk mitigation and recovery efforts for networked information systems

CS

Assertions to be proven

- CI is a network of networks
- CIP protects the network of networks
- CIP networks share data/ information

The role of standards

- Interoperability
  - Semantic and syntactic
  - Interconnect
- Safety
- Governance
  - Radio resources
  - Numbering/addressing space
- Correctness and accuracy

Standards as market creators

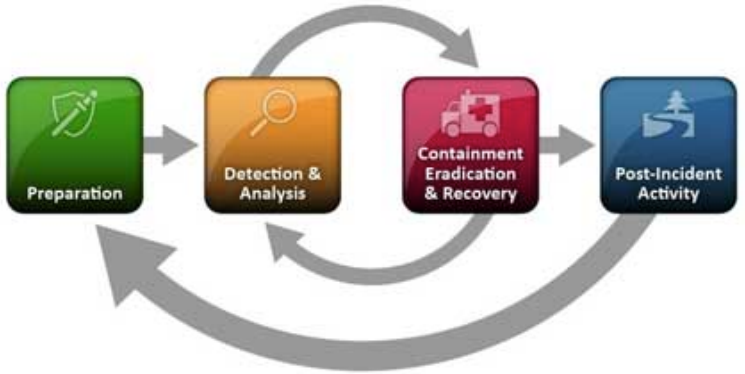
- Fosters collaborative competition
- Enables markets with multiple players
- Enables market diversification without demanding lock in
- Notably successful model
  - 7 billion cellular phone users (>93% global penetration, some countries have >100% penetration) http://wdi.worldbank.org/table/5.11

ICT in Critical Infrastructures

- It is clear to most casual observers that the global economic infrastructure is now composed of a huge set of ICT networks and services.
  - ICT capabilities underpin all of the other critical infrastructures:
    - Food security, economic activity security, citizen safety, transport, power generation and distribution, health, logistics, the emergency services, citizen information, …
- Role of ESTI and other SDOs in CI:
  - Resilience (from ENISA report); Supply chain integrity (from ENISA report); M2M communications and IoT; eHealth; Critical event communications; …

Standards and security in CI analysis

- Not so very different from any other security analysis
  1. Detect
     - Part of the preparation phase in which we need to detect a potential problem. What do we need to detect?
  2. Report
     - Share knowledge.
  3. Respond
     - Contain, Eradicate, Recover



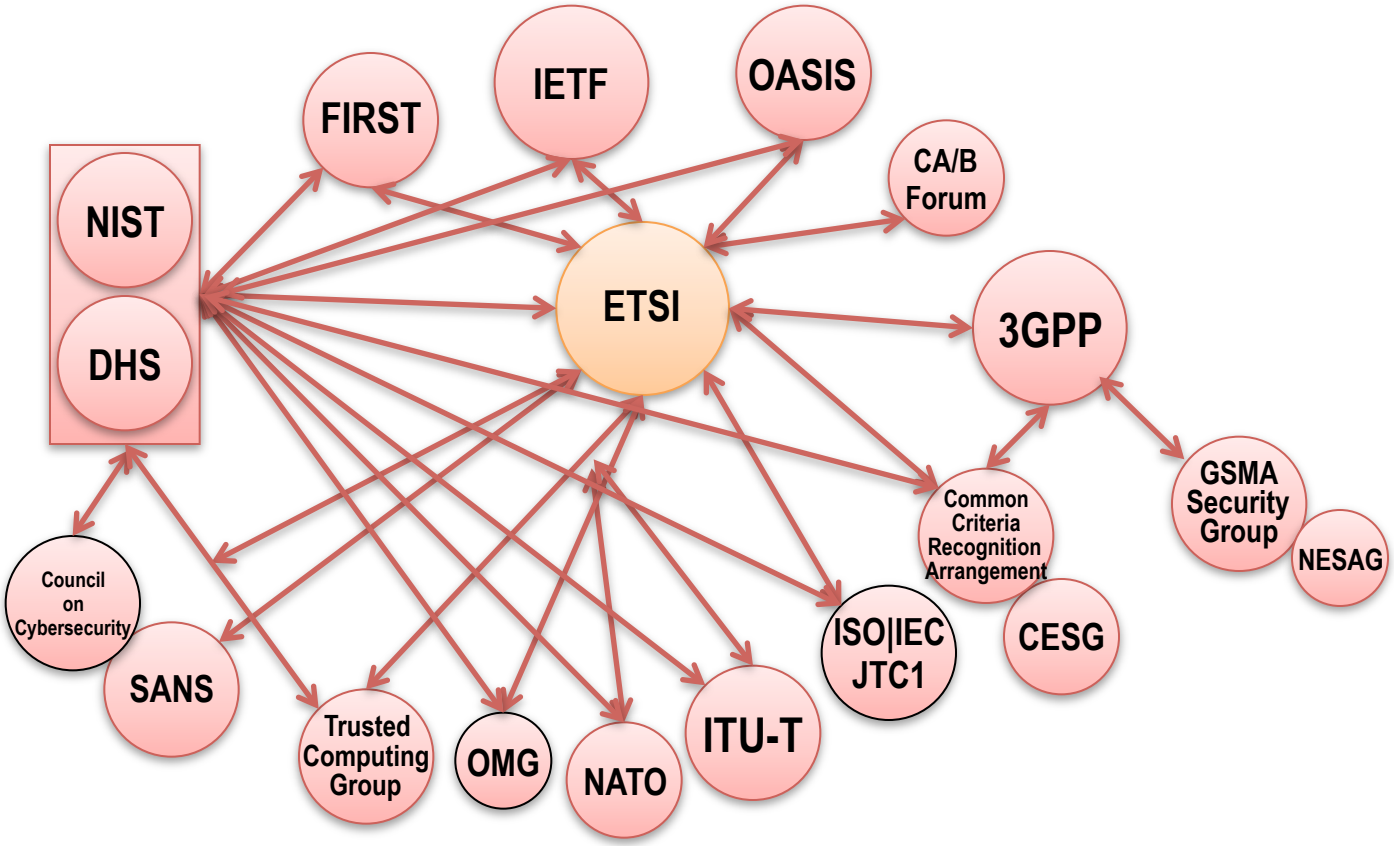
ETSI Clusters

http://www.etsi.org/technologies-clusters/clusters

Standards in CI? In CIP?

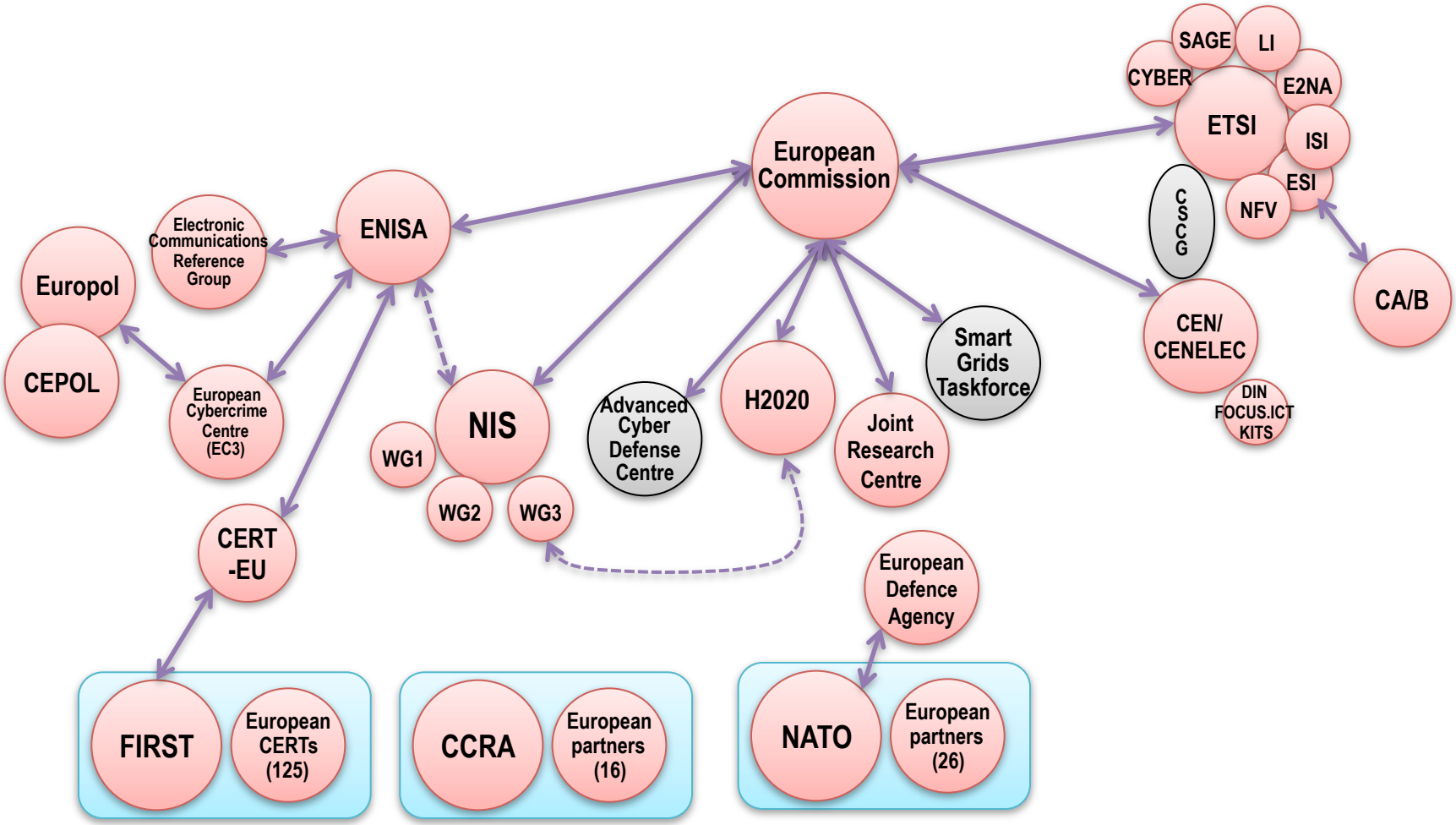
- Disaster response?
  - TETRA and Critical Communications Evolution
- CI reporting?
  - smartM2M, oneM2M, Cyber, STIX, CERTs, …
- Infrastructure protection?
  - 3GPP-SA3, TCCE-6, ITS-5, CYBER, M2M-SEC, …

Cyber Security SDO ecosystem



The ETSI TR 103 306 “Global Cyber Security Ecosystem “ regularly updated in order to follow the constantly evolving global Cyber Security scenario

European Cyber Security ecosystem



Areas of security standardization

- Cyber Security
- Mobile/Wireless Comms (GSM/UMTS, TETRA, DECT…)
- Lawful Interception and Data Retention
- Electronic Signatures
- Smart Cards
- Machine-to-Machine (M2M)
- Methods for Testing and Specification (MTS)
- Emergency Communications / Public Safety
- RFID
- Intelligent Transport Systems
- Information Security Indicators
- Quantum Key Distribution (QKD)
- Identity and access management for Networks and Services (INS)
- Algorithms
- In 3GPP

ETSI TC CYBER

- Cyber Security Standardization
- Security of infrastructures, devices, services and protocols
- Security advice, guidance and operational security requirements to users, manufacturers and network and infrastructure operators
- Security tools and techniques to ensure security
- Creation of security specifications and alignment with work done in other TCs and ISGs
- Coordinate work with external groups such as the CSCG with CEN, CENELEC, the NIS Platform and ENISA
- Collaborate with other SDOs (ISO, ITU, NIST, ANSI...)
- Answer to policy requests on Cyber Security and ICT security in broad sense

TC CYBER meetings

- TC CYBER has met 3 times face-to-face
  - Around 50 participants at each meeting
- Rapporteurs also develop work items through teleconference
  - 10 to 20 technical participants per call
- Participating organizations
  - Industry: Manufacturers, Operators, SMEs...
  - Administrations
  - European Commission
  - ENISA
  - Universities / Research Bodies
  - Service Providers
  - Micro Enterprises

TC CYBER work items in development

- 9 open documents
  - 8 Technical Reports
  - 1 ETSI Guide

- TR 103 303, Protection measures for ICT in the context of Critical Infrastructure
- TR 103 304, PII Protection and Retention
- TR 103 305, Security Assurance by Default; Critical Security Controls for Effective Cyber Defence
- TR 103 306, Global Cyber Security Ecosystem
- TR 103 307, Security Aspects for LI and RD interfaces
- TR 103 308, A security baseline regarding LI for NFV and related platforms
- TR 103 309, Secure by Default adoption – platform security technology
- TR 103 331, Structured threat information sharing
- EG 203 310, Post Quantum Computing Impact on ICT Systems

International Collaboration in ETSI

- TC CYBER to create/keep relations with other ETSI TCs/ISGs
- CYBER as leading ETSI security body
- Reference for any other TC and technology
- Reference for Liaisons with other Standard Developing Organisations (SDOs)

TC: Technical Committee

ISG: Industry Specification Group

CSCG (Cyber Security Coordination Group)

- Advisory Body of the three ESOs (CEN/CENELEC/ETSI)
- Composed of ESO members and EU institutions
  - CCMC, ETSI, ENISA, JRC, DG ENTR
- White Paper Feb 2014: 9 main Recommendations for a Strategy on European Cyber Security Standardization

CSCG 9 Recommendations (in 3 main areas)

- **GOVERNANCE**
  - Coordination, scope, trust
- **HARMONISATION**
  - PKI/cryptography, requirements/evaluation, EU security label, interface with research
- **GLOBALISATION**
  - Harmonisation with international key players, global promotion of EU Cyber Security standards
- CSCG currently working on the Recommendations
  - Definition of actions and responsibilities

Security Week (at ETSI premises)

- Workshop, Technical Streams, Meetings
  - Including TC CYBER#4 Meeting
- Workshop/Streams free and open to everyone
  - CI and CIP will be addressed in many of the streams
- TC CYBER meeting open to non ETSI Members upon invitation (see website to apply)
- **www.etsi.org/securityweek**
  - Agendas and registrations
- Separate registrations to events

Security Week

	Mon 22	Tue 23	Wed 24	Thu 25	Fri 26
AM		**Workshop**	**Workshop**	**CYBER#4** **ISI#23** eIDAS	**CYBER#4**
PM	**Workshop**	**Workshop**	**Streams:** M2M/IoT ITS eIDAS HF/USER/ eHealth	**CYBER#4** **ISI#23** eIDAS	**CYBER#4**

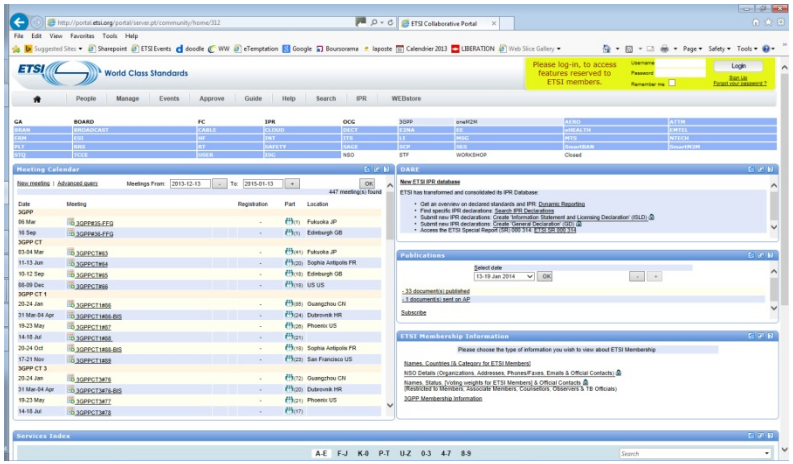
- M2M/IoT: Machine-to-Machine / Internet of Things
- ITS: Intelligent Transport Systems
- eIDAS: Electronic identification and trust services
- HF: Human Factors
- USER: User Group
- eHealth: Health ICT

ETSI on the web

- ETSI website *(http://www.etsi.org)*
  - General public information
  - **Free** standards download (~30000)
  - Promotional aspects

- ETSI portal *(http://portal.etsi.org)*
  - Easy access to data for each Technical Body
  - Working documents
  - ETSI applications and databases

- 3GPP website *(www.3gpp.org)*



- Forapolis website *(www.forapolis.org)*

Please keep in touch!

Contact Details:

scott@cadzow.com

Thank you!
Available for your questions