Welcome to the World of Standards

ETSI

World Class Standards

CYBERSECURITY

Overview of Cybersecurity

Presented by Charles Brookson ETSI TC CYBER Chairman **for** Brussels Sept 2017

ABOUT ETSI CYBERSECURITY

Brief facts

- ETSI, the European Telecommunications Standards Institute, produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies. Our standards enable the technologies on which business and society rely.
- For example, our standards for GSM™, DECT™, Smart Cards and electronic signatures

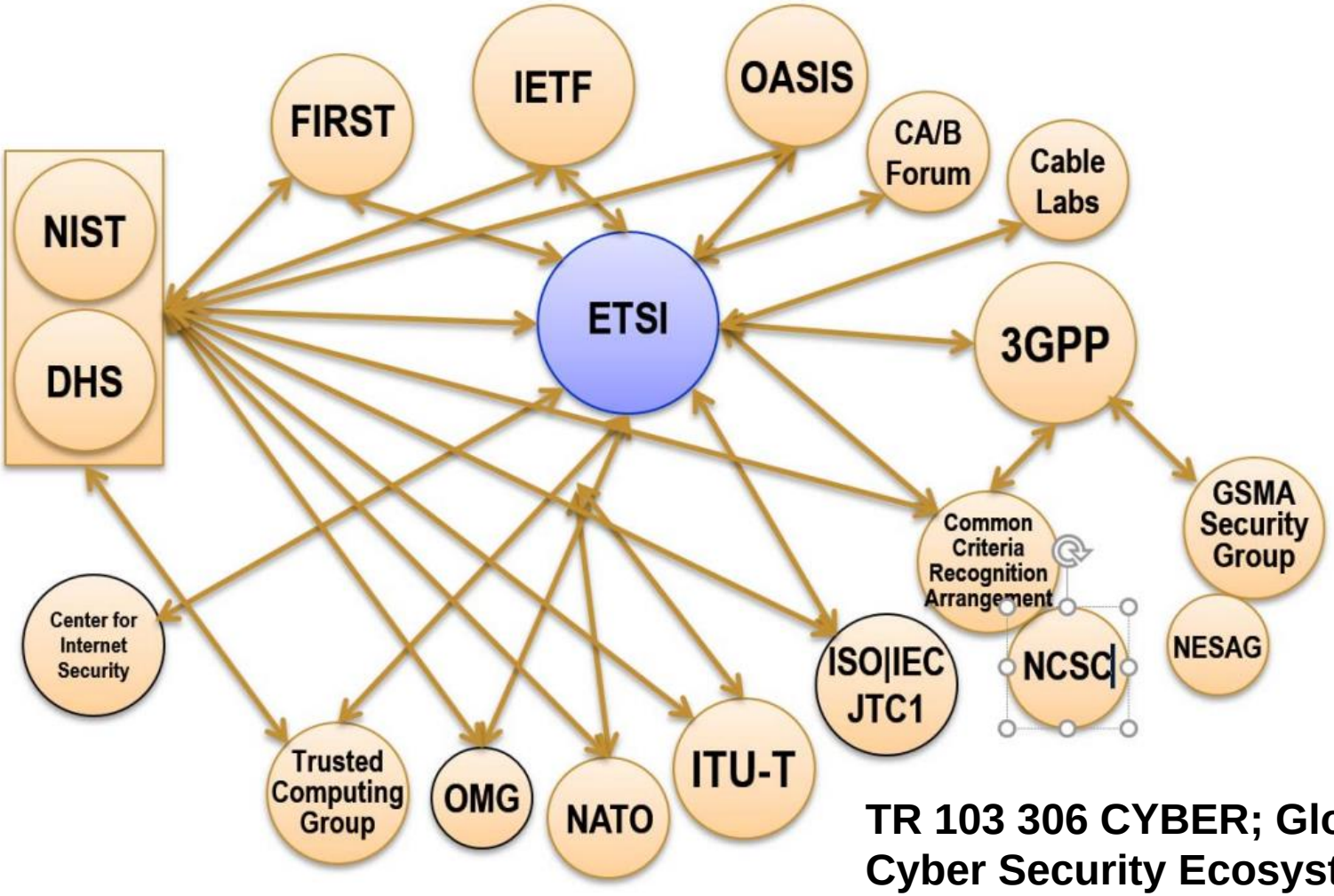
About ETSI

- We have been doing Cybersecurity for a long time …
  - Security since 1988
  - Annual report http://www.etsi.org/about/annual-report
- Areas of security
  - The Internet of Things
  - eHealth
  - Trust Service Providers
  - Secure Cards and Elements
  - Cryptography
  - Network Functions Virtualization
  - Lawful Interception and Data Retention

CYBERSECURITY

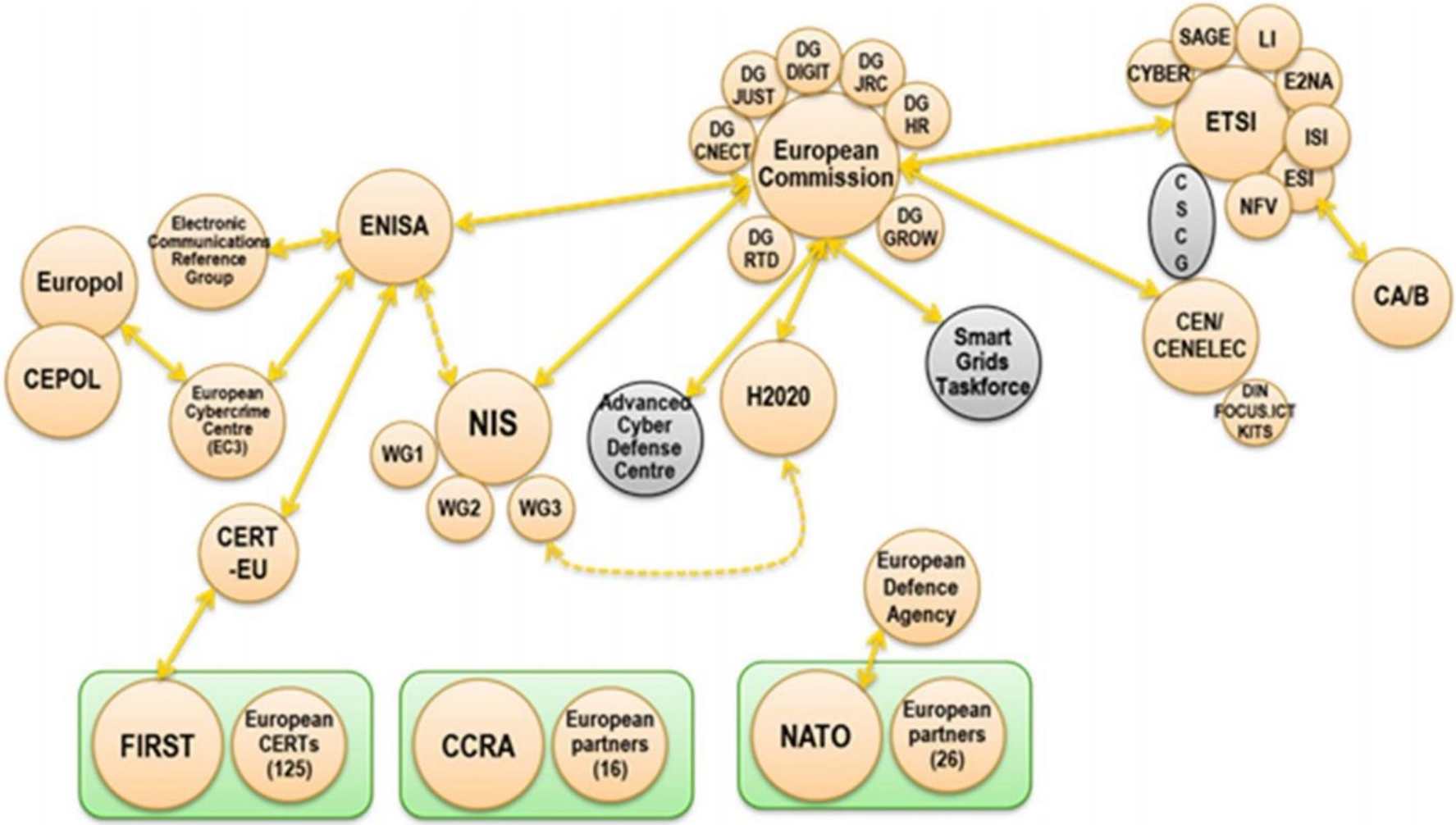
Activities

Cybersecurity worldwide



TR 103 306 CYBER; Global Cyber Security Ecosystem

Cybersecurity within Europe



ETSI role

- TC CYBER sets base standards for ETSI and provides expertise where required:
  - Security white paper
    - http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp18_CyberSecurity_Ed1_FINAL.pdf
  - Role, Standards
    - http://www.etsi.org/technologies-clusters/technologies/cyber-security

Cyber Security at ETSI

- Horizontal cybersecurity
  - Global Cybersecurity Ecosystem
  - Privacy by design
  - Security controls
  - Information Security Indicators
  - Network and Information Security
  - Network gateway cyber defence and middlebox security…
- Securing technologies and systems
  - Mobile/Wireless Comms (3G/4G, TETRA, DECT, RRS, RFID…)
  - IoT and Machine-to-Machine (M2M)
  - Network Functions Virtualisation
  - Intelligent Transport Systems
  - Broadcast…
- Security tools and techniques
  - Lawful Interception and Retained Data
  - Digital Signatures and trust service providers
  - Secure elements
  - Cryptography (algorithms, quantum key distribution, quantum-safe cryptography)

Key Technical concerns

- Privacy by Design
  - Building information in from the start
- The Sharing of Cyber Threat Intelligence
  - Sharing information
- Statistics and Metrics
  - Analyzing cyber threats
- Securing Technologies and Systems
  - Mobile communications (3GPP), NFV, Future Networks, Intelligent Transport Systems, Digital Enhanced Cordless Telecommunications (DECT™), M2M communications and emergency telecommunications (including Terrestrial Trunked Radio (TETRA)). These technologies are dealt with primarily within dedicated technical committees.

ETSI working on Security Standardization

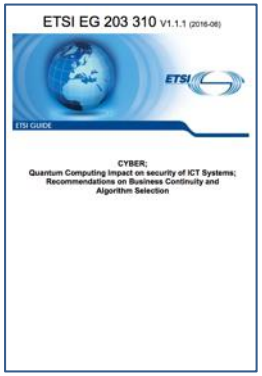
- The Internet of Things
- eHealth
- Trust Service Providers
- Secure Cards and Elements
- Cryptography
- Network Functions Virtualization
- Lawful Interception and Data Retention
- Security within work areas

NIS Directive

- TR 103 456 Implementation of the Network and Information Security (NIS) Directive *Publication soon this year*
  - Guidance on available and ongoing standards or development initiatives to meet Directive (EU) 2016/1148
  - Overview of the NIS Directive
    - The context for NIS
    - ENISA recommendations on standardisation
  - Cyber threat intelligence sharing: incidents and risks
  - Role of risk analysis in protecting NIS
  - Challenges, obstacles, and recommendations
  - Harmonizing implementations across the diverse network and service sectors and Member State legal and operational environments
  - Recommendations

Example of Guide on Quantum Computing

- EG 203 310 Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection
  - In brief if the promise of quantum computing holds true then the following impacts will be immediate on the assumption that the existence of viable quantum computing resources will be used against cryptographic deployments:
    - Symmetric cryptographic strength will be halved, e.g. AES with 128 bit keys giving 128 bit strength will be reduced to 64 bit strength (in other words to retain 128 bit security will require to implement 256 bit keys).
    - Elliptical curve cryptography will offer no security.• RSA based public key cryptography will offer no security.
    - The Diffie-Helman-Merkle key agreement protocol will offer no security.


ETSI EG 203 310 V1.1.1 (2016-08)

ETSI GUIDE

CYBER;
Quantum Computing Impact on security of ICT Systems;
Recommendations on Business Continuity and
Algorithm Selection

Standards of TC CYBER

- TR 103 421 CYBER; Network Gateway Cyber Defence
- TR 103 306 CYBER; Global Cyber Security Ecosystem
- TS 103 307 CYBER; Security Aspects for LI and RD Interfaces
- TR 103 305-1 CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls
- TR 103 305-2 CYBER; Critical Security Controls for Effective Cyber Defence; Part 2: Measurement and auditing
- TR 103 305-3 CYBER; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations
- TR 103 305-4 CYBER; Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms
- TR 103 331 CYBER; Structured threat information sharing
- TR 103 304 CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services
- TR 103 369 CYBER; Design requirements ecosystem
- EG 203 310 CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection
- TS 103 307 CYBER; Security Aspects for LI and RD Interfaces
- TR 103 303 CYBER; Protection measures for ICT in the context of Critical Infrastructure
- TS 103 487 CYBER; Baseline security requirements regarding sensitive functions for NFV and related platforms
- TR 103 308 CYBER; Security baseline regarding LI and RD for NFV and related platforms
- TR 103 306 CYBER; Global Cyber Security Ecosystem
- TR 103 309 CYBER; Secure by Default - platform security technology
- TR 103 305 CYBER; Critical Security Controls for Effective Cyber Defence

Contacts

Contact Details:

ETSI www.etsi.org

Charles Brookson ETSI TC CYBER Chairman

charles@zeata.co.uk

Thank you!