

2nd Indo-European Dialogue on ICT Standards & Emerging Technologies

4th November 2015 • Shangri-La's - Eros Hotel, New Delhi, INDIA



Cybersecurity

Presented by Charles Brookson OBE CEng FIET FRSA

Cybersecurity overview

Looking at the work around the world



2nd Indo-European Dialogue on
ICT Standards & Emerging Technologies

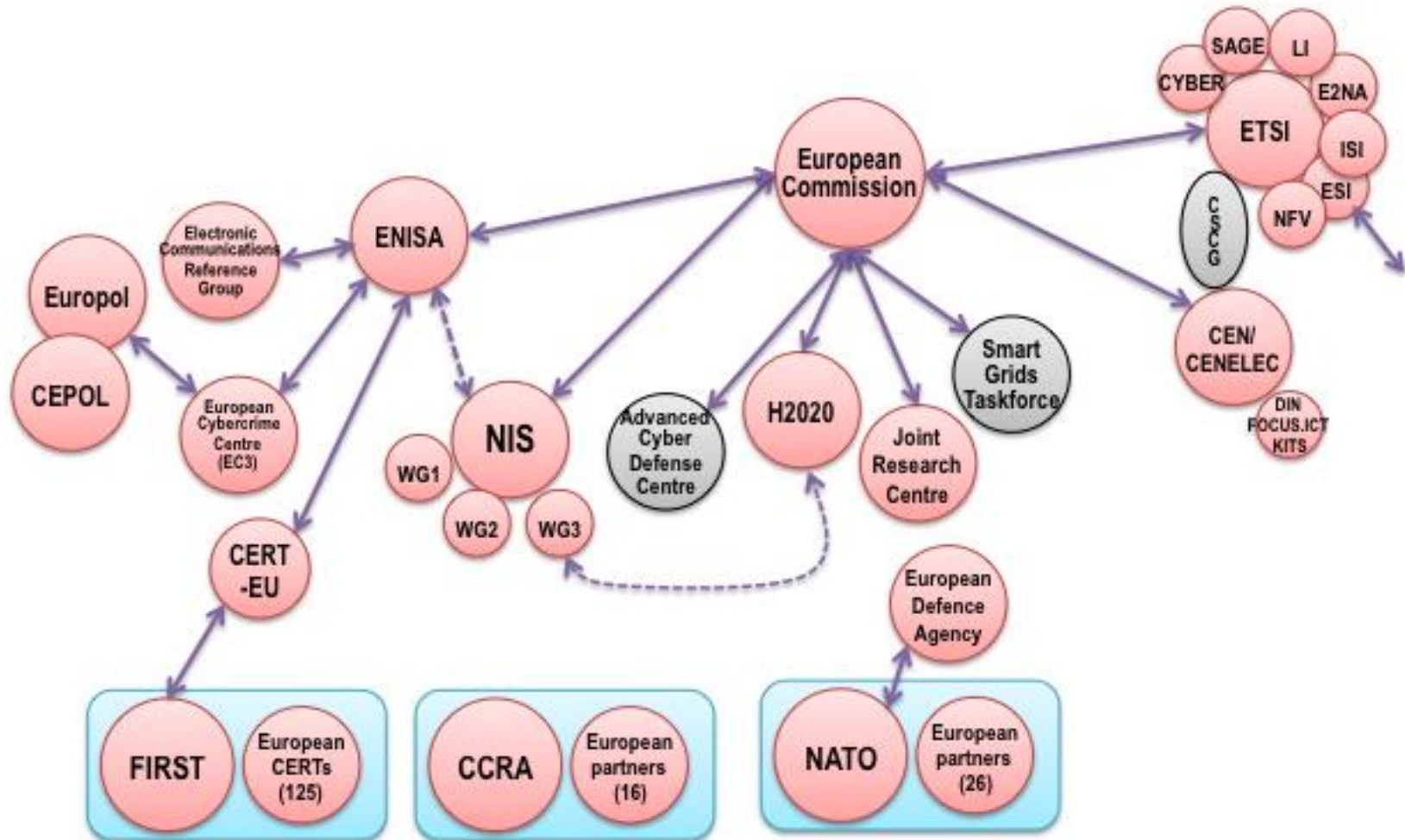
4th November 2015 • Shangri-La's - Eros Hotel, New Delhi, INDIA

What is Cybersecurity?

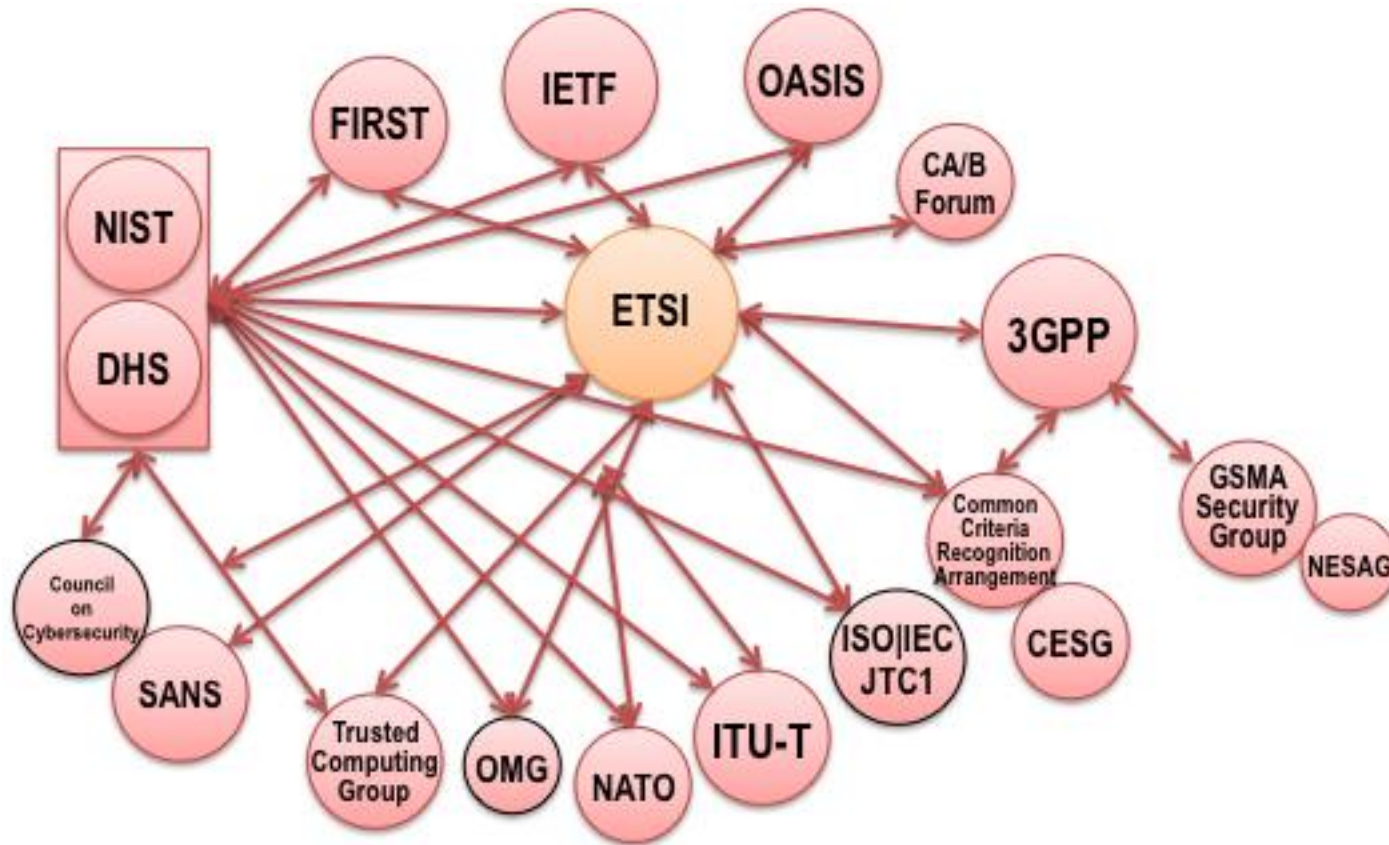
- ❖ Many definitions!!
- ❖ Security of:
 - ❖ Systems, Devices, Networks, Infrastructure
 - ❖ Can extend to Information, Data.
- ❖ NIST says
 - ❖ Cybersecurity – The ability to protect or defend the use of cyberspace from cyber attacks.
 - ❖ Cyberspace – A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.



European Eco System



World Eco System



Council on Cybersecurity Top Twenty Controls

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defenses
6. Application Software Security
7. Wireless Device Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Protection
18. Incident Response and Management
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises

*The Critical Security Controls for Effective Cyber Defense Version 5.0

<http://www.counciloncybersecurity.org/attachments/article/12/CSC-MASTER-VER50-2-27-2014.pdf>



CESG (UK Government) 10 Steps to Risk Management

- ❖ Information risk management regime
- ❖ Secure configuration
- ❖ Network security
- ❖ Managing user privileges
- ❖ User education & awareness
- ❖ Incident management
- ❖ Malware protection
- ❖ Monitoring
- ❖ Removable media controls
- ❖ Home & mobile working



3GPP SA3 SECAM and GSMA SG NESAG

❖ 3GPP SA3 (Security)

❖ Established SECAM: Study on Security Assurance Methodology for 3GPP network products

❖ Technical specifications with security requirements and corresponding test cases collected in a document named SAS (Security Assurance Specification)

❖ Follows Common Criteria model

❖ GSMA Security Group

❖ Established a new Network Equipment Security Assurance Group (NESAG)

❖ Complements SECAM on the administrative framework and Accreditation Body aspects



NIST Cybersecurity Framework and Roadmap

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NIST Roadmap for Improving Critical Infrastructure Cybersecurity

Areas for Development, Alignment, and Collaboration

- Authentication
- Automated Indicator Sharing
- Conformity Assessment
- Cybersecurity Workforce
- Data Analytics
- Federal Agency Cybersecurity Alignment
- International Aspects, Impacts and Alignment
- Supply Chain Risk Management
- Technical Privacy Standards

<http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf>

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, 12 February 2014 <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>



Cybersecurity in ETSI

Looking at ETSI



2nd Indo-European Dialogue on
ICT Standards & Emerging Technologies

4th November 2015 • Shangri-La's - Eros Hotel, New Delhi, INDIA

ETSI TC CYBER

- ❖ Working with CEN and CENELEC (CSCG)
 - ❖ Feb 2014 CSCG provided Recommendations for a Strategy on European Cyber Security Standardization
 - ❖ 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)
- ❖ Receives Directives from EC - Examples
 - ❖ Network and Information Security,
 - ❖ Privacy.
- ❖ Works with other Standards bodies
 - ❖ ISO, ITU-T, 3GPP, NIST etc.



ETSI TC CYBER – Terms of Reference

- ❖ 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



Security in ETSI – 1

- ❖ Mobile and Wireless telecommunication
 - ❖ GSM, UMTS, LTE
 - ❖ TETRA
 - ❖ DECT
- ❖ Satellite
- ❖ Radio Frequency Identification - RFID
- ❖ Reconfigurable Radio Systems - RRS
- ❖ Intelligent Transport Systems - ITS
- ❖ Machine to Machine - M2M
- ❖ Lawful Interception
- ❖ Electronic Signatures
- ❖ Algorithms



Security in ETSI – 2

- ❖ Identify and Access Management for Networks and Services
- ❖ Information Security Indicators - ISI
- ❖ Smart Cards
- ❖ Future Networks
- ❖ Emergency and Public Safety Telecommunications - EMTEL - MESA
- ❖ Aeronautics
- ❖ Maritime



Security in ETSI – 3

- ❖ Network Functions Virtualisation - NFV
- ❖ Quantum Key Distribution
- ❖ Quantum Safe Cryptography
- ❖ Broadcasting
- ❖ Media Content Distribution
- ❖ Security Testing
- ❖ IPv6
- ❖ ePassport Readers
- ❖ IPCablecomm



TC CYBER Work Items

- ❖ 13 documents (2 published, 1 approved for publication)
 - ❖ 9 Reports, 3 Specifications, 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 (published and under revision)
- ❖ TR 103 306, Global Cyber Security Ecosystem (approved, to be published soon)
- ❖ TS 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 (published)
- ❖ TR 103 369, Design requirements ecosystem
- ❖ TR 103 370, Practical introductory guide to privacy
- ❖ TR 103 331, Structured threat information sharing
- ❖ EG 203 310, Post Quantum Computing Impact on ICT Systems
- ❖ TS 103 485, Mechanisms for privacy assurance and verification
- ❖ TS 103 486, Identity management and naming schema protection mechanisms



Finally!

Looking at the ways we can work together



2nd Indo-European Dialogue on
ICT Standards & Emerging Technologies

4th November 2015 • Shangri-La's - Eros Hotel, New Delhi, INDIA

Together

- ❖ Read our information
 - ❖ *Use the useful information for yourselves*
- ❖ Work together to:
 - ❖ Highlight issues, gaps, improvement, stop duplication
 - ❖ Areas of common interest
 - ❖ Raise Work Items?
- ❖ Co-operation agreement?



TC CYBER Reference material

- ❖ TC CYBER on ETSI portal and ToR
 - ❖ <https://portal.etsi.org/cyber>
 - ❖ https://portal.etsi.org/cyber/Cyber_ToR.asp
- ❖ ETSI Security White Paper
 - ❖ 7th Edition Published January 2015
 - ❖ Achievements, ongoing work, list of publications
 - ❖ www.etsi.org/securitywhitepaper



Contact details

❖ Charles Brookson – TC CYBER Chairman

❖ charles@zeata.co.uk

❖ Carmine (Lino) Rizzo – TC CYBER Technical Officer

❖ carmine.rizzo@etsi.org

