National Committee for Cyber Security, Resilience and Business Continuity for Electrical Grids

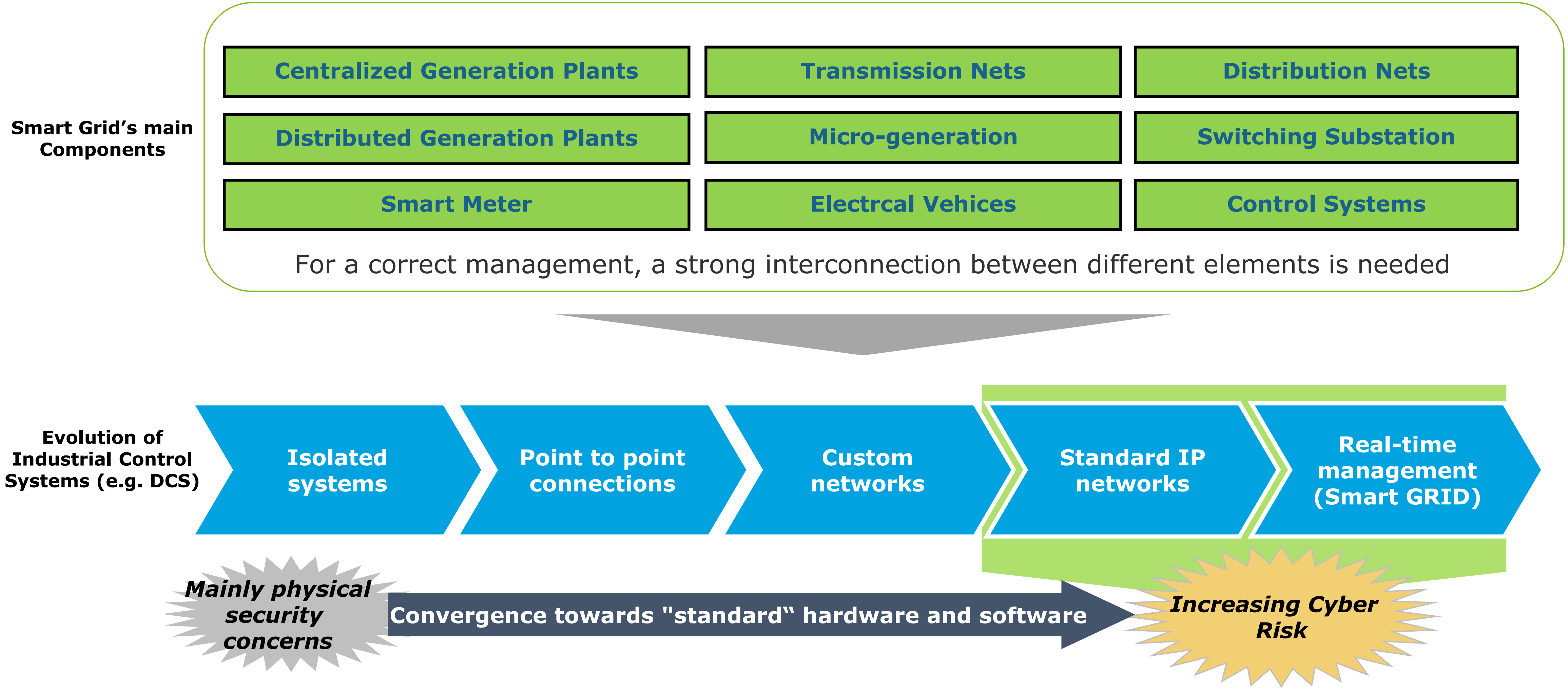
President: Prof. Paola Girdinio – Università degli Studi di Genova - DITEN –Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni (Department of Naval, Electronic, Electric and TeleCommunications Engineering)

Security Officer: Dr. Antonio Rebora - Ansaldo Energia SpA
Business Continuity & Crisis Management: Gianna Detoni – PANTA RAY

St. Petersburg – September 28 2017

The growing integration between the IT and OT world is of outstanding importance in relation to the management of smart grids. On the other hand, it has introduced cyber risks within the whole electrical field/sector.

The IT-OT integration versus Cyber Risk



Smart Grid's main Components

Centralized Generation Plants	Transmission Nets	Distribution Nets
Distributed Generation Plants	Micro-generation	Switching Substation
Smart Meter	Electrcal Vehices	Control Systems

For a correct management, a strong interconnection between different elements is needed

Evolution of Industrial Control Systems (e.g. DCS)

- Isolated systems
- Point to point connections
- Custom networks
- Standard IP networks
- Real-time management (Smart GRID)

Mainly physical security concerns

Convergence towards "standard‟ hardware and software

Increasing Cyber Risk

Due to this development, managers are asked to raise awareness on how cyber threats can affect the business and the service supply

Electricity Sector Worldwide Cyber Security Threat Landscape

Threat Actor Examples: Dragonfly / Energetic Bear

Action Period	✦ 2011 - 2017	**Targets**	✦ Energy grid, production company and Industrial Solutions suppliers including ICS ✦ 84 nation affected, particularly US, Spain, France, Italy, Germany, Turkey e Poland
Description	An hacking group from Eastern Europe focusing mainly on sabotage and espionage		

Examples:

Significant Cyber Security Accidents

Shamoon Attack - Saudi Aramco

Attacker	Cutting Sword of Justice
Discovery date	August 2012
Target	Political sabotage
Impact	✦ 35,000 hard drives partially / totally destroyed ✦ IT services offline ✦ 5 months for a full recovery

BlackEnergy Power Grid in Ucraina

Attacker	Unknown
Discovery date	December 2015
Target	Political sabotage
Impact	✦ Completely acquisition of the remote control of HMI, SCADA, power backup and telco systems ✦ 230,00 resident citizens offline for hours (best case) or days (worst case)

Ransomware Attack - Utility[1], Michigan USA

Attacker	Unknown
Discovery date	April 2016
Target	Financial (Ransom)
Impact	✦ Spear phishing attack with malware inoculation ✦ Self-forced stop of all company systems for two weeks

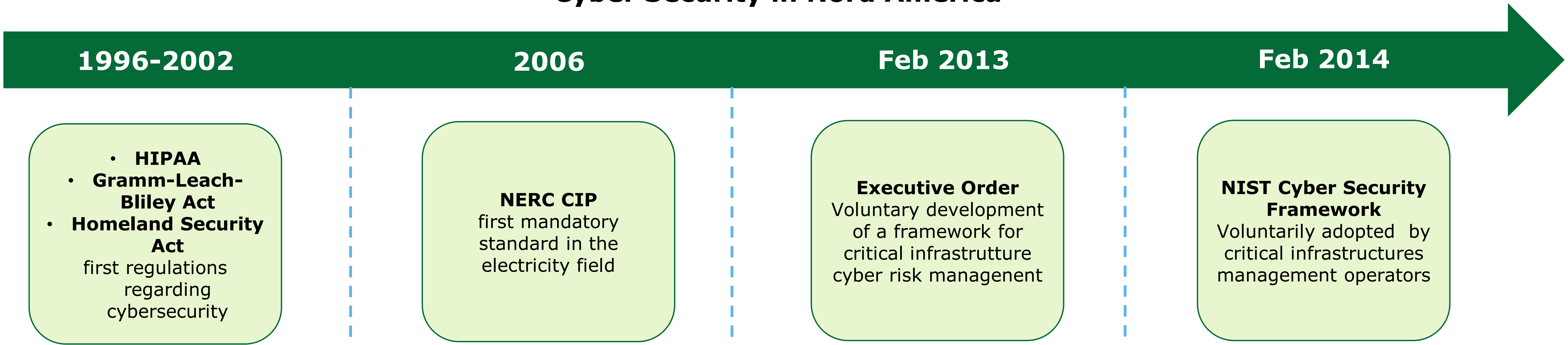
DDOS Attack - DYN Domain Name System

Attacker	Unknown
Data Scoperta	October 2016
Target	Vandalism
Impact	✦ DDOS attack from about "ten million" of malware infected IoT ✦ Amazon, PayPal, Twitter, Netflix, Spotify and other off-line for several hours

[1] Lansing Board of Water and Light, Lansing, Michigan USA

In the mid-1990’s , North America started to develop field regulations for the Cyber Security management, which eventually turned out into structural frameworks.

Cyber Security in Nord America



1996-2002

- **HIPAA**
- **Gramm-Leach-Bliley Act**
- **Homeland Security Act**

first regulations regarding cybersecurity

2006

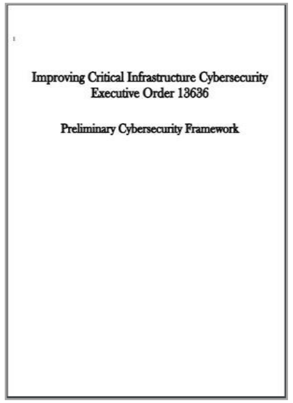
NERC CIP
first mandatory standard in the electricity field

Feb 2013

Executive Order
Voluntary development of a framework for critical infrastrutture cyber risk managenent

Feb 2014

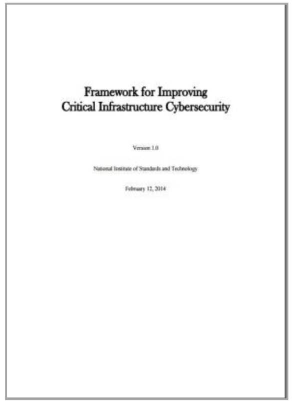
NIST Cyber Security Framework
Voluntarily adopted by critical infrastructures management operators



1

Improving Critical Infrastructure Cybersecurity
Executive Order 13636

Preliminary Cybersecurity Framework



Framework for Improving
Critical Infrastructure Cybersecurity

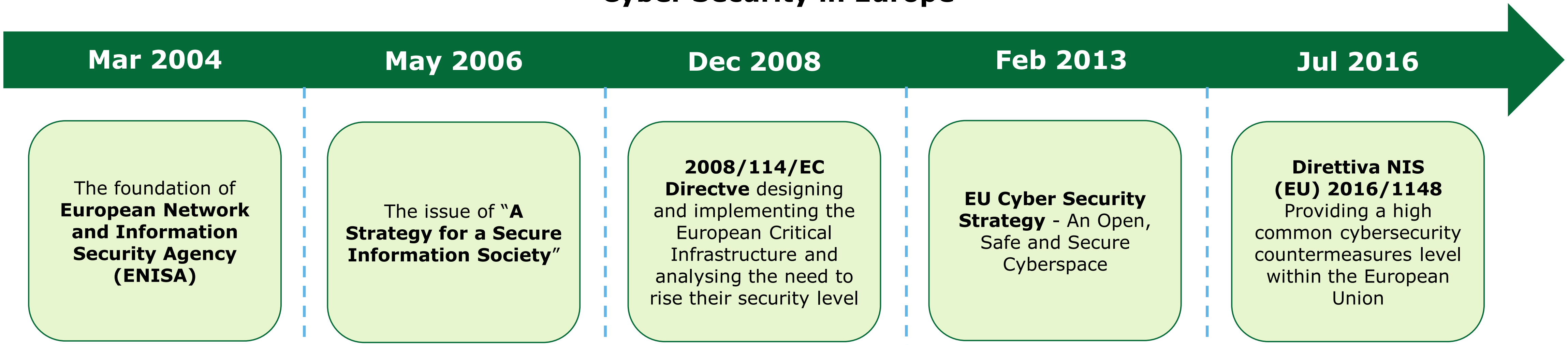
Version 1.0

National Institute of Standards and Technology

February 12, 2014

Since 2004, Europe has been provided with increasingly developed organisms, strategies, and regulations in order to increase and improve the management of Cyber Security topics.

Cyber Security in Europe



Mar 2004

The foundation of **European Network and Information Security Agency (ENISA)**

May 2006

The issue of "**A Strategy for a Secure Information Society**"

Dec 2008

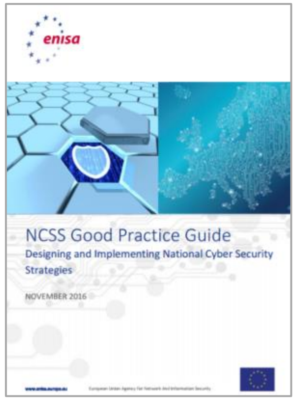
2008/114/EC Directve designing and implementing the European Critical Infrastructure and analysing the need to rise their security level

Feb 2013

EU Cyber Security Strategy - An Open, Safe and Secure Cyberspace

Jul 2016

Direttiva NIS (EU) 2016/1148 Providing a high common cybersecurity countermeasures level within the European Union



enisa

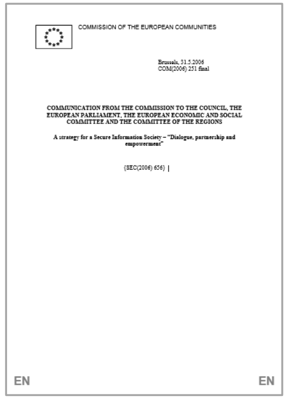
NCSS Good Practice Guide

Designing and Implementing National Cyber Security Strategies

NOVEMBER 2016

www.enisa.europa.eu

European Union Agency For Network And Information Security



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 31.5.2006
COM(2006) 251 final

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"

{SEC(2006) 656}

EN EN

23.12.2008 EN Official Journal of the European Union L 345/75

COUNCIL DIRECTIVE 2008/114/EC

of 8 December 2008

on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

(Text with EEA relevance)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 308 thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Parliament [1],

[illegible]

EUROPEAN COMMISSION

HIGH REPRESENTATIVE OF THE EUROPEAN UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY

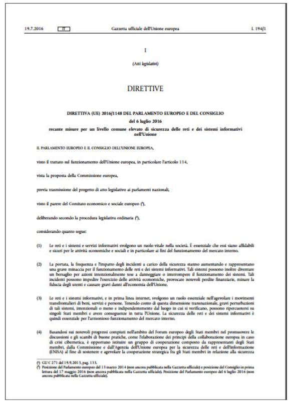
Brussels, 7.2.2013
JOIN(2013) 1 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Cybersecurity Strategy of the European Union:

An Open, Safe and Secure Cyberspace

EN EN



19.7.2016 IT Gazzetta ufficiale dell'Unione europea L 194/1

I

(Atti legislativi)

DIRETTIVE

DIRETTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 6 luglio 2016

recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

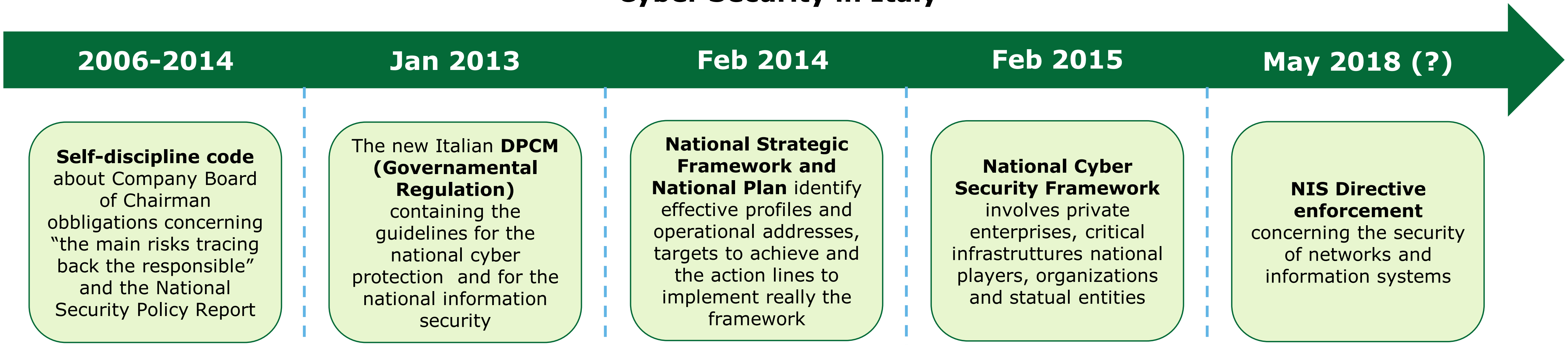
visto il parere del Comitato economico e sociale europeo [1],

deliberando secondo la procedura legislativa ordinaria [2],

[illegible]

Since 2014 Italy has been experiencing a strong speed-up as far as Cyber Security is concerned, while in the next few months further steps ahead are likely to occur.

Cyber Security in Italy



2006-2014

Self-discipline code about Company Board of Chairman obbligations concerning “the main risks tracing back the responsible” and the National Security Policy Report

Jan 2013

The new Italian **DPCM (Governamental Regulation)** containing the guidelines for the national cyber protection and for the national information security

Feb 2014

National Strategic Framework and National Plan identify effective profiles and operational addresses, targets to achieve and the action lines to implement really the framework

Feb 2015

National Cyber Security Framework involves private enterprises, critical infrastruttures national players, organizations and statual entities

May 2018 (?)

NIS Directive enforcement concerning the security of networks and information systems

Presidenza del Consiglio dei Ministri
Sistema di informazione per la sicurezza della Repubblica

RELAZIONE
SULLA POLITICA DELL’INFORMAZIONE
PER LA SICUREZZA

2015

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 gennaio 2013.

Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale.

Pubblicato nella G.U. 19 marzo 2013, n. 66.

IL PRESIDENTE DEL CONSIGLIO DEI Ministri

Vista la *legge 3 agosto 2007, n. 124*, recante "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto", come modificata e integrata dalla *legge 7 agosto 2012, n. 133*, e, in particolare, l'*art. 1*, comma 3-bis, che dispone che il Presidente del Consiglio dei Ministri, sentito il Comitato interministeriale per la sicurezza della Repubblica, adotti apposite direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, e l'*art. 38*, comma 1-bis, ai sensi del quale il Governo allega alla relazione sulla politica dell'informazione per la sicurezza e sui risultati ottenuti, che presenta annualmente al Parlamento, un documento di sicurezza nazionale, concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali, nonché alla protezione cibernetica e alla sicurezza informatica;

Visto l'*art. 4, comma 3, lett. d-bis) della citata legge 3 agosto 2007, n. 124*, ai sensi del quale il Dipartimento delle informazioni per la sicurezza coordina le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali;

Visto l'*articolo 1 della legge 1° aprile 1981, n. 121*;

Visti il *decreto-legge 27 luglio 2005, n. 144*, convertito, con modificazioni, dalla *legge 31 luglio 2005, n. 155*, recante misure urgenti per il contrasto del terrorismo internazionale che, all'*articolo 7-bis*, dispone che, ferme restando le competenze dei Servizi di informazione per la sicurezza, i competenti organi del Ministero dell'interno assicurano i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale ed il *decreto del Ministro dell'interno 9 gennaio 2008*, con il quale sono state individuate le predette infrastrutture ed è stata prevista l'istituzione del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche;

Visti l'*art. 14 del decreto legislativo 30 luglio 1999, n. 300*, recante "Riforma dell'organizzazione del Governo, a norma dell'*articolo 11 della legge 15 marzo 1997, n. 59*", che attribuisce, tra l'altro, al Ministero dell'interno competenze in materia di difesa civile ed il decreto del Ministro dell'interno 28 settembre 2001 che istituisce la Commissione interministeriale tecnica di difesa civile;

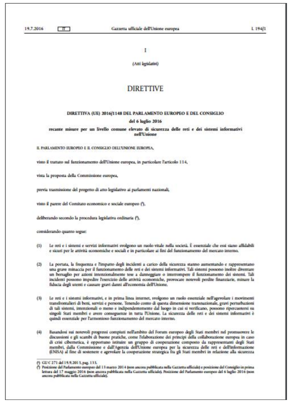
QUADRO
PER LA SI
DELLO SI

Presidenza del Consiglio dei Ministri

PIANO NAZIONALE
PER LA PROTEZIONE CIBERNETICA
E LA SICUREZZA INFORMATICA

2015 Italian Cyber Security Report

Cyber Security National Lab



19.7.2016 IT Gazzetta ufficiale dell'Unione europea L 194/1

I

(Atti legislativi)

DIRETTIVE

DIRETTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 6 luglio 2016

recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo [1],

deliberando secondo la procedura legislativa ordinaria [2],

considerando quanto segue:

(1) Le reti e i sistemi e servizi informativi svolgono un ruolo vitale nella società. È essenziale che essi siano affidabili e sicuri per le attività economiche e sociali e in particolare ai fini del funzionamento del mercato interno.

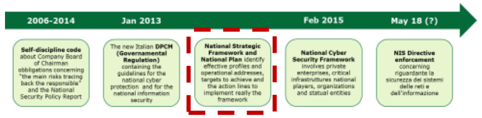
(2) La portata, la frequenza e l'impatto degli incidenti a carico della sicurezza stanno aumentando e rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi. Tali sistemi possono inoltre diventare un bersaglio per azioni intenzionalmente tese a danneggiare o interrompere il funzionamento dei sistemi. Tali incidenti possono impedire l'esercizio delle attività economiche, provocare notevoli perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia dell'Unione.

(3) Le reti e i sistemi informativi, e in prima linea internet, svolgono un ruolo essenziale nell'agevolare i movimenti transfrontalieri di beni, servizi e persone. Tenendo conto di questa dimensione transnazionale, gravi perturbazioni di tali sistemi, intenzionali o meno e indipendentemente dal luogo in cui si verificano, possono ripercuotersi su singoli Stati membri e avere conseguenze in tutta l'Unione. La sicurezza delle reti e dei sistemi informativi è quindi essenziale per l'armonioso funzionamento del mercato interno.

(4) Basandosi sui notevoli progressi compiuti nell'ambito del Forum europeo degli Stati membri nel promuovere le discussioni e gli scambi di buone pratiche, come l'elaborazione dei principi della collaborazione europea in caso di crisi cibernetica, è opportuno istituire un gruppo di cooperazione composto da rappresentanti degli Stati membri, dalla Commissione e dall'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) al fine di sostenere e agevolare la cooperazione strategica fra gli Stati membri in relazione alla sicurezza

[1] GU C 271 del 19.9.2013, pag. 133.
[2] Posizione del Parlamento europeo del 13 marzo 2014 (non ancora pubblicata nella Gazzetta ufficiale) e posizione del Consiglio in prima lettura del 17 maggio 2016 (non ancora pubblicata nella Gazzetta ufficiale). Posizione del Parlamento europeo del 6 luglio 2016 (non ancora pubblicata nella Gazzetta ufficiale).

The Italian National Strategic Framework, amongst others, encourages the partnership between public and private sector



2006-2014 — **Self-discipline code** about Company Board of Chairman obbligations concerning "the main risks tracing back the responsible" and the National Security Policy Report

Jan 2013 — The new Italian **DPCM (Governamental Regulation)** containing the guidelines for the national cyber protection and for the national information security

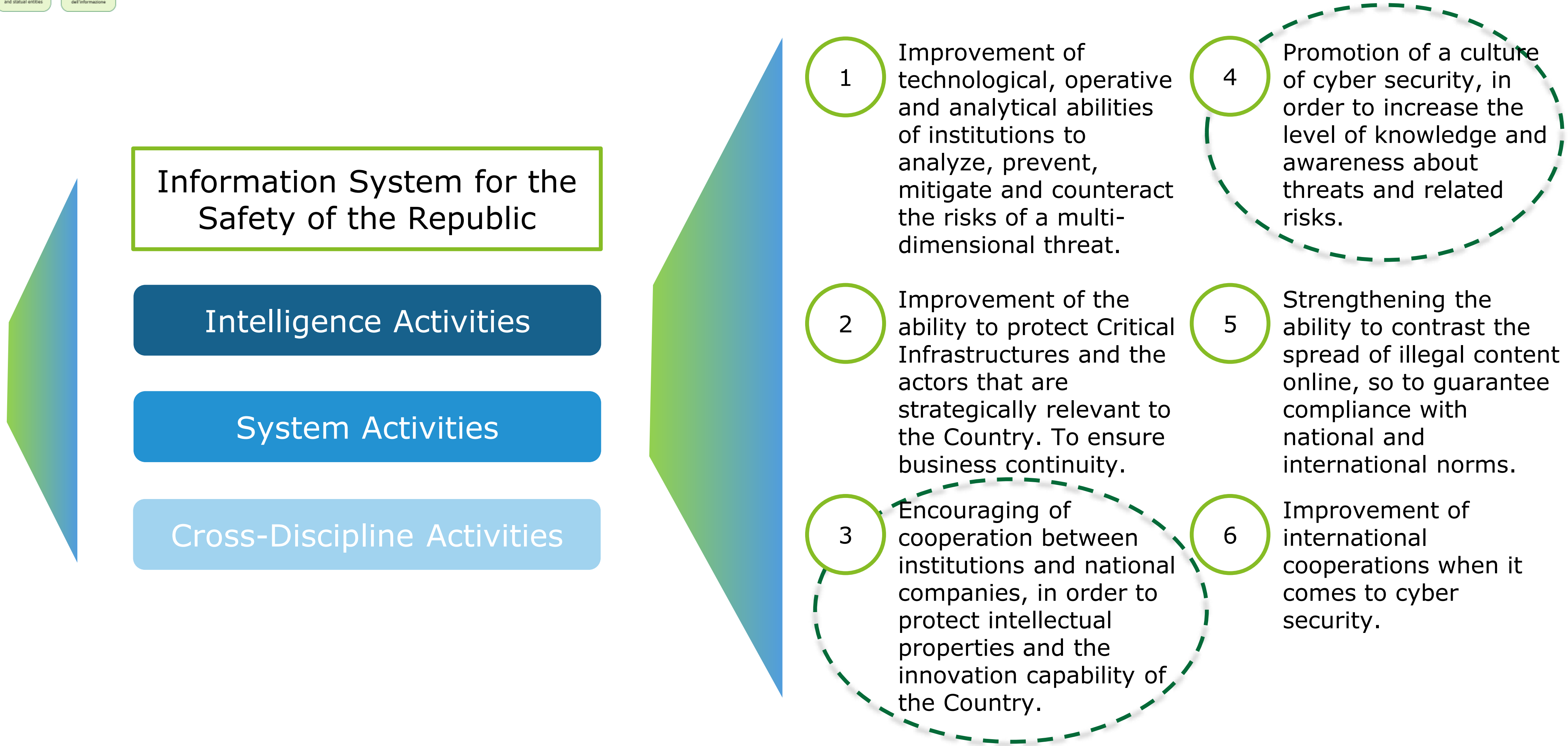
National Strategic Framework and National Plan identify effective profiles and operational addresses, targets to achieve and the action lines to implement really the framework

Feb 2015 — **National Cyber Security Framework** involves private enterprises, critical infrastruttures national players, organizations and statual entities

May 18 (?) — **NIS Directive enforcement** concerning riguardante la sicurezza dei sistemi delle reti e dell'informazione

National Strategic Framework

Presidenza del Consiglio dei Ministri
QUADRO STRATEGICO NAZIONALE PER LA SICUREZZA DELLO SPAZIO CIBERNETICO
Dicembre 2013



Information System for the Safety of the Republic

Intelligence Activities

System Activities

Cross-Discipline Activities

1 Improvement of technological, operative and analytical abilities of institutions to analyze, prevent, mitigate and counteract the risks of a multi-dimensional threat.

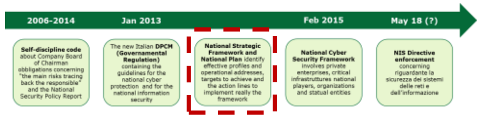
2 Improvement of the ability to protect Critical Infrastructures and the actors that are strategically relevant to the Country. To ensure business continuity.

3 Encouraging of cooperation between institutions and national companies, in order to protect intellectual properties and the innovation capability of the Country.

4 Promotion of a culture of cyber security, in order to increase the level of knowledge and awareness about threats and related risks.

5 Strengthening the ability to contrast the spread of illegal content online, so to guarantee compliance with national and international norms.

6 Improvement of international cooperations when it comes to cyber security.



2006-2014

Self-discipline code about Company Board of Chairman obbligations concerning "the main risks tracing back the responsible" and the National Security Policy Report

Jan 2013

The new Italian **DPCM (Governamental Regulation)** containing the guidelines for the national cyber protection and for the national information security

National Strategic Framework and National Plan identify effective profiles and operational addresses, targets to achieve and the action lines to implement really the framework

Feb 2015

National Cyber Security Framework involves private enterprises, critical infrastruttures national players, organizations and statual entities

May 18 (?)

NIS Directive enforcement concerning riguardante la sicurezza dei sistemi delle reti e dell'informazione

National Strategic Framework

Presidenza del Consiglio dei Ministri

PIANO NAZIONALE
PER LA PROTEZIONE CIBERNETICA
E LA SICUREZZA INFORMATICA

Dicembre 2013

1. Improvement of intelligence agencies, and civil and military defense capabilities
2. **Improvement of the organization and the methodologies of coordination and interaction between public and private entities**
3. Promotion and spread of a culture of information security. Teaching and training
4. International cooperation and exercises
5. Operations of national CERT, CERT-PA and local CERTs
6. Legislative action and compliance with international standards
7. Compliance with standards and safety protocols
8. Support to the industrial and technological development
9. Strategic communication
10. Resources
11. Implementation of a national Information Risk Management system

The norms, and particularly the partnership private-public sector and the involvement of the academic world, inspired the creation of the Committee

National Committee for Cyber Security of Electrical Grids

VISION

The National Committee for Cyber Security, Resilience and Business Continuity of Electrical Grids has the objective to develop an instrument which allows for 1) an integrated management of cyber security, 2) the creation and promotion of collaboration initiatives, 3) information exchange and research in the field of electric energy grids**, through the involvement of both public and private entities.**

STRUCTURE

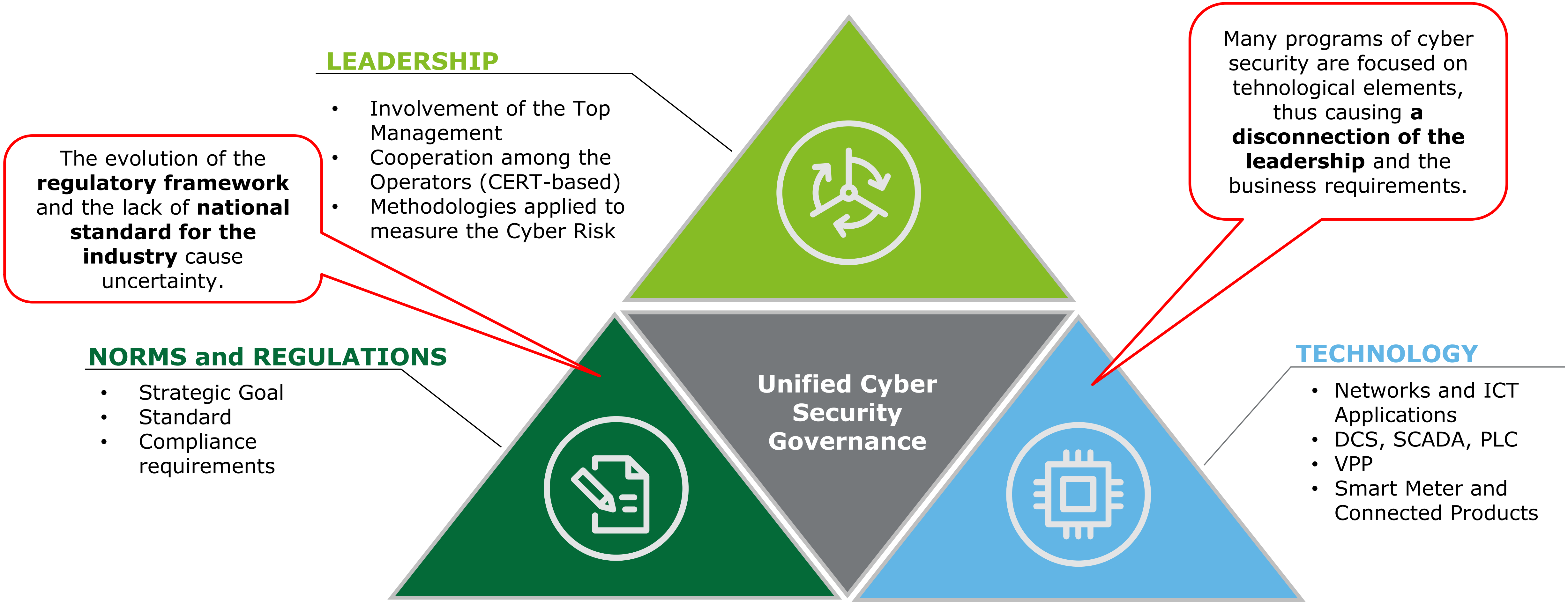
The permanent working table formed in 2015 performs its activities regarding all the national Critical Electric Infrastructures and all the levels of the national system of Generation, Transmission and Distribution (AT/MT/BT), with particular attention to new assets of Cyber Security of the modern National grid, which presents more and more Green and Smart Grid elements.

The working table of the Committee has numerous collaborations and contributions, starting from the Scuola Politecnica of Engineering of the University of Genova, to the biggest national players of electric energy, such as ENEL, ANSALDO Energia, TERNA, IREN and others. In addition to them, there are also providers of systems and products which support the grids, such as Leonardo, Kaspersky, Siemens, ABB, and others.

Contacts with companies and entities that operate on the national territory; PANTA RAY, Intellium-Deloitte, MAPS Group, GCSEC.

The Committee has the objective to facilitate the development of a framework that will assist the Italian Operators in the electricity field in managing effectively the Cyber Security challenges

Main challenges for the Electrical Companies



LEADERSHIP

- Involvement of the Top Management
- Cooperation among the Operators (CERT-based)
- Methodologies applied to measure the Cyber Risk

Many programs of cyber security are focused on tehnological elements, thus causing **a disconnection of the leadership** and the business requirements.

The evolution of the **regulatory framework** and the lack of **national standard for the industry** cause uncertainty.

NORMS and REGULATIONS

- Strategic Goal
- Standard
- Compliance requirements

Unified Cyber Security Governance

TECHNOLOGY

- Networks and ICT Applications
- DCS, SCADA, PLC
- VPP
- Smart Meter and Connected Products

The first step is the identification of the methodologies that will enable the involvement of the Top Management, facilitating a common language among people with a different background…

Key Cyber Security Actors

Key Cyber Security Actors	**Top Management**	**Enterprise Risk Management (ERM)**	**Information and Communications Technology (ICT)**	**Industrial Control Systems (ICS)**
Typical Background	**MBA**	**Audit / Security**	**Electronics / Communications**	**Industrial Process Engineering**
Daily Terminology	• Profit and Loss • Balance Sheet • Stakeholder Relations • Marketing Strategy	• Business Impact Analysis • COSO Model • SOX Compliance • Supply and Demand Risks	• IAM • TCP / IP • OSI Model • ISO 27001/2 (ISMS)	• Regasification • Purdue Model • HAZOPs • ISA / IEC 62443
Typical Vendors	• McKinsey & Co • Bain & Co • Boston Consulting Group	• Big 4 Auditors • EMC / RSA / Archer • SAS Analytics	• Microsoft • IBM / HP • SAP	• ABB • Honeywell • Emerson
Primary Concerns	• Overall Business Success	• Optimized Risk Portfolio	• Information Confidentiality, Integrity, and Availability	• Personnel Safety • Process Efficiency / Availability

...and define a common methodology to introduce to the board members all the cyber risks identified in the IT and OT

Example of a methodology for the Cyber Risk Management

Cyber Security Risk Management ICT e ICS

Level of risk evaluation for the three paramethers: Confidentiality (C), Integrity (I), Availability (A).

Coordinamento tra le funzioni

Impact analysis, both for IT and OT, facilitating the cooperation among the organization’s functions, aiming to identify the systems’ relationship and interconnections.

Metodologia comune

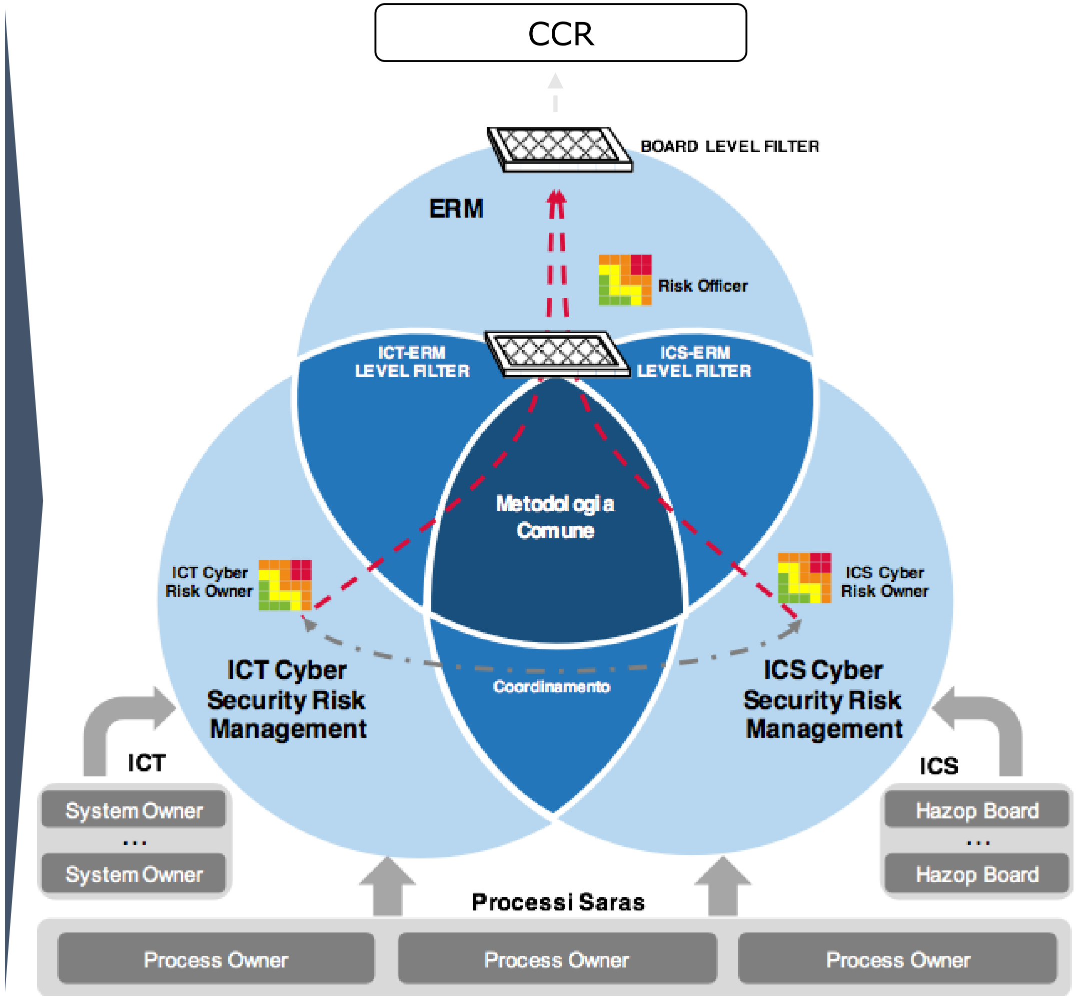
Alignment with the ERM methodology to enable a comparison among the levels of Cyber risk with the other risks managed in the Enterprise

Metodo di selezione rischi ICT / ICS

Definition of tools to present to the Risk Officer a clear overviwe of the risks connected to the IT and OT world.

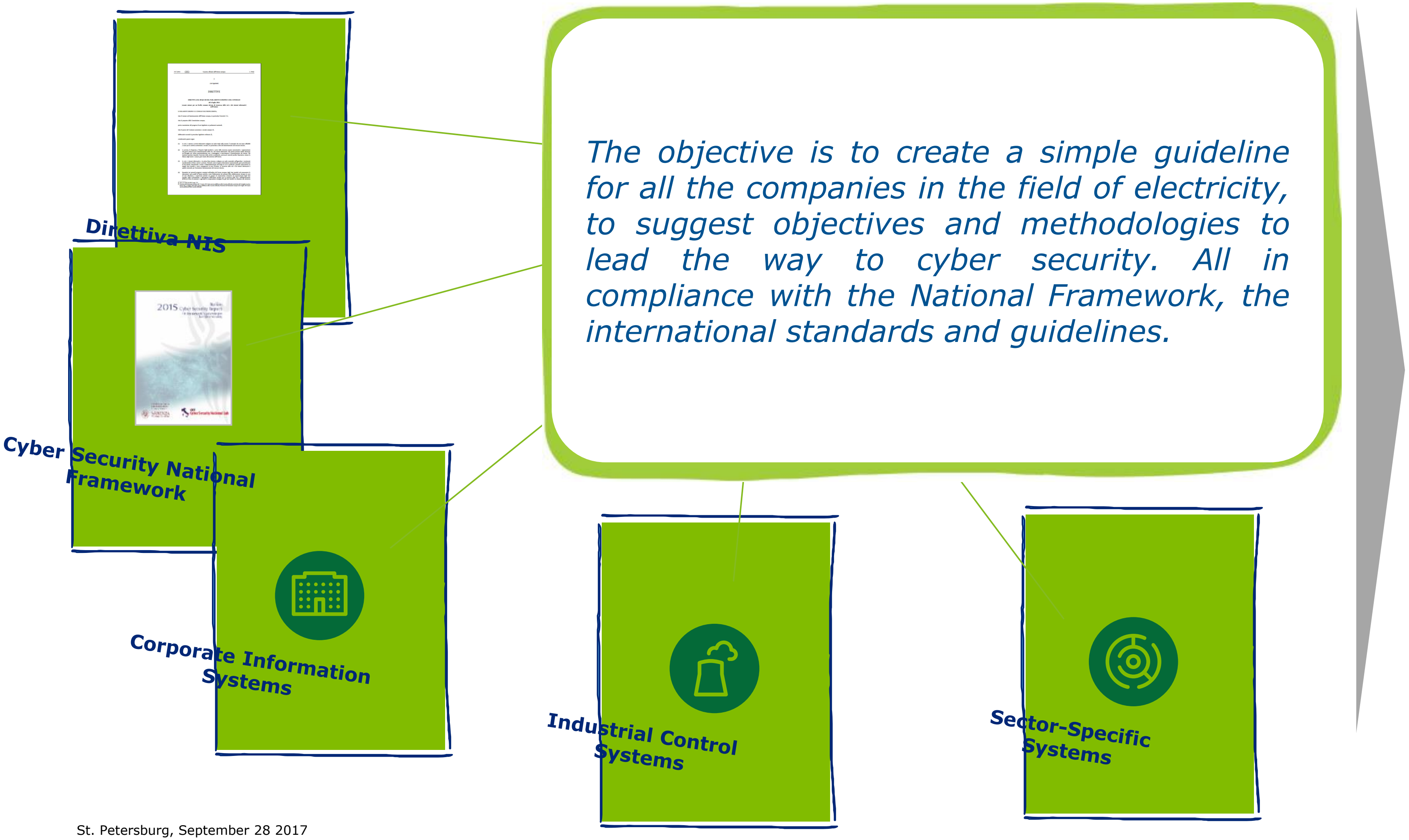
Presentazione al Board

Presentation to the CCR of the main risks only. The elements managed at the Enterprise level are filtered considering only those that are within the predefined ‘Risk Appetite’.



Defining Principles, Guidelines and Best Practices for the management of cyber security and in compliance with European and national norms

Guidelines


Direttiva NIS
Cyber Security National Framework
Corporate Information Systems
Industrial Control Systems
Sector-Specific Systems

The objective is to create a simple guideline for all the companies in the field of electricity, to suggest objectives and methodologies to lead the way to cyber security. All in compliance with the National Framework, the international standards and guidelines.

Guidelines

Part 1 – Recommendations for the management of Cyber Security

- What is Cyber Security and the normative framework
- Approach to Cyber Security in the Electricity field
- Role of Top Management in Cyber Risk Management
- Business continuity and risk management
- Computer Emergency Readiness Team (CERT)
- Development of a Cyber Security Programme Governance
- Required resources
- Training
- Management of Service Providers

Part 2 – Notes for implementation

- Implementation of measures in the context of critical infrastructures in the field of electricity
- Notes for the implementation of NIST CORE Framework

In order to support the operators of the electricity field in the management of cyber security topics, the Committee defined an action plan based on 5 key points

Action Plan of the Committee

01 **…defining a National Framework for Cyber Security**

02 **…helping Top Management to handle cyber risk**

03 **…developing a capability of Incident Response**

04 **…promoting Information-Sharing**

05 **…improving Business Continuity and Cyber Readiness…**

…through the collaboration and cooperation of Public Entities, Academies, Technology Producers and Experts of Cyber Security

National Committee for Cyber Security, Resilience and Business Continuity for Electrical Grids

President: Prof. Paola Girdinio – Università degli Studi di Genova - DITEN –Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni (Department of Naval, Electronic, Electric and TeleCommunications Engineering)

Security Officer: Dr. Antonio Rebora - Ansaldo Energia SpA
Business Continuity & Crisis Management: Gianna Detoni – PANTA RAY

St. Petersburg – September 28 2017