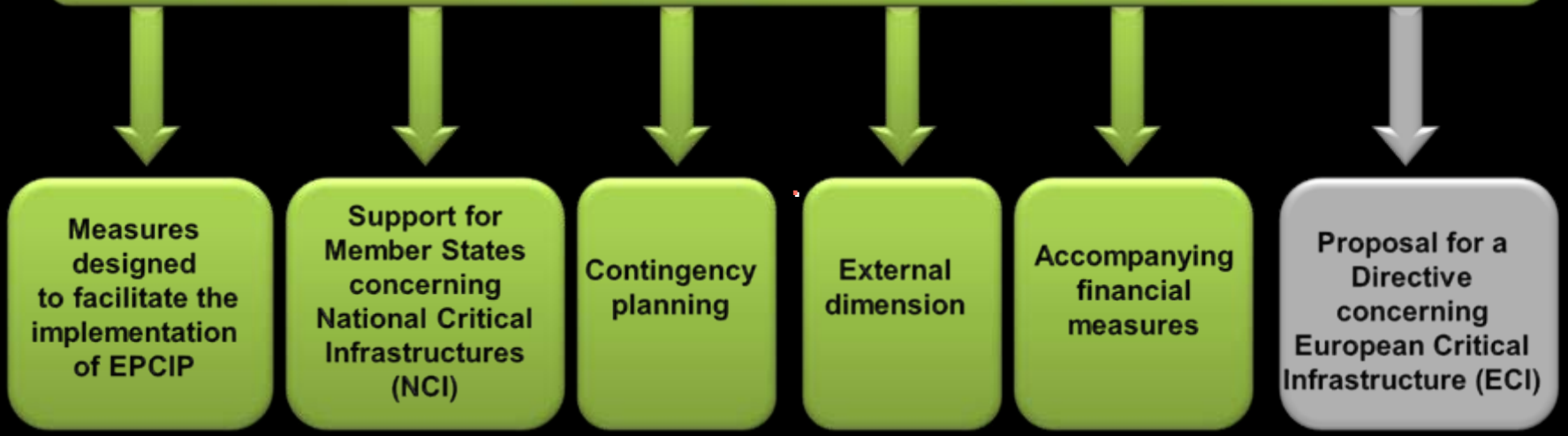
Infrastrutture Critiche e ICT: situazione in Italia e in Europa

Ing. Luisa Franchina
Direttore Generale
Segreteria Infrastrutture Critiche

Ufficio del Consigliere Militare
Presidenza del Consiglio dei Ministri

The European Programme for Critical Infrastructure Protection Framework

Countering threats from terrorism is a priority, but the programme encompass an all hazards approach (i.e. terrorist attacks and natural disasters alike) Protection measures should be: Affordable; Sustainable; Reliable and Proportionate



- EPCIP Action Plan
- Critical Infrastructure Warning Information Network (CIWIN)
- CIP expert groups
- CIP information sharing
- identification and analysis of interdependencies

EU programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013

A procedure for the identification and designation of ECI

A common approach to the assessment of the needs to improve the protection of such infrastructures

Definition of Critical Infrastructure

From Directive 114/08 EC

“Critical Infrastructure” means those assets, systems or parts thereof located in the EU Member States which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions;

Infrastructure

From Directive 114/08 EC

“European Critical Infrastructure” means critical infrastructure located in the EU Member States the disruption or destruction of which would have a significant impact on at least two Member States of the EU. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure;

Art. 3

Pursuant to the procedure provided in Annex III, each Member State shall identify potential ECIs which both satisfy the cross-cutting and sectoral criteria and meet the definitions set out in Article 2(a) and (b).

……

The cross-cutting criteria referred to shall comprise the following:

(a) **casualties** criterion (assessed in terms of the potential number of fatalities or injuries);

(b) **economic effects** criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);

(c) **public effects** criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services).

…….

The cross-cutting criteria **thresholds** shall be based on the **severity of the impact of the disruption or destruction** of a particular infrastructure

From Risk analysis to Impact analysis

Risk = *f* (Threat, Vulnerability, worst Exposure)

$Impact_{event}$

- real “exposure” at “ground zero” (victims, economics, pub. consequences, …)
- effectiveness of the attack
- effectiveness of the reaction

$Impact_{domino}$

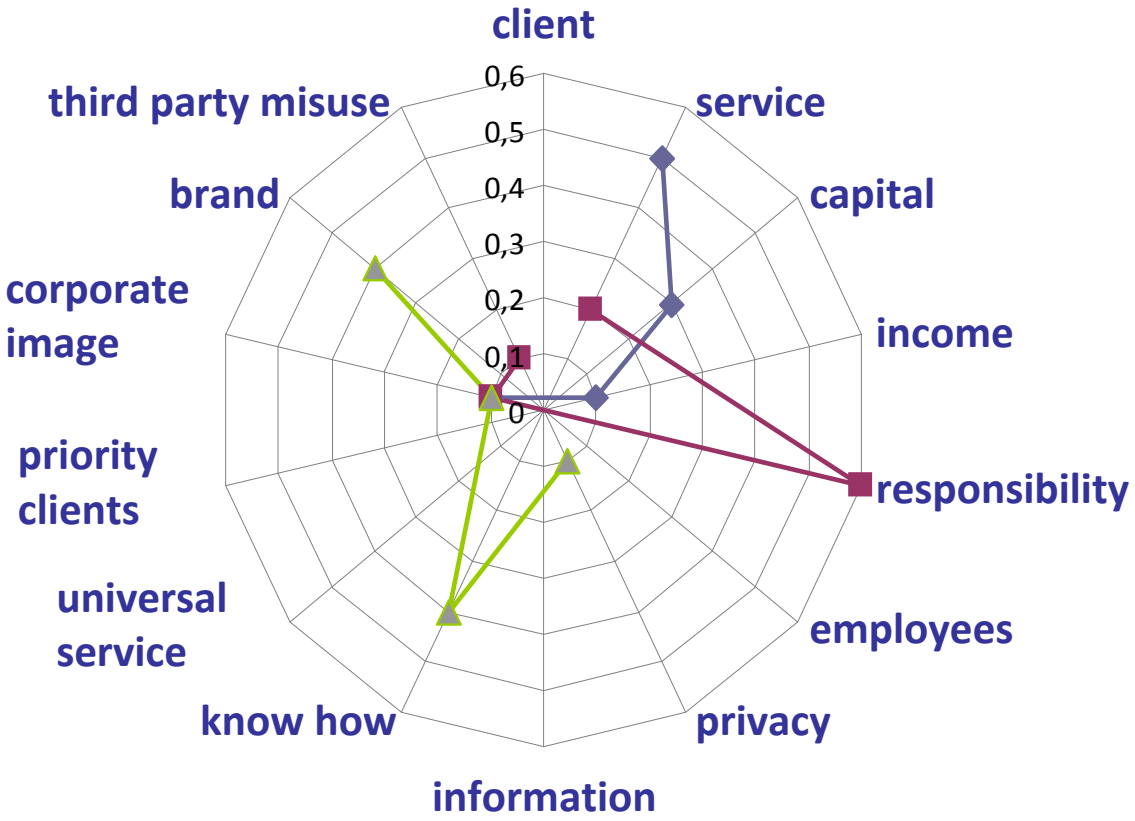
- sum of consequences of outage of CIs involved in the domino effect (victims, economics, pub. consequences, …)
- “mitigation” factors

Criteria (direct and indirect)

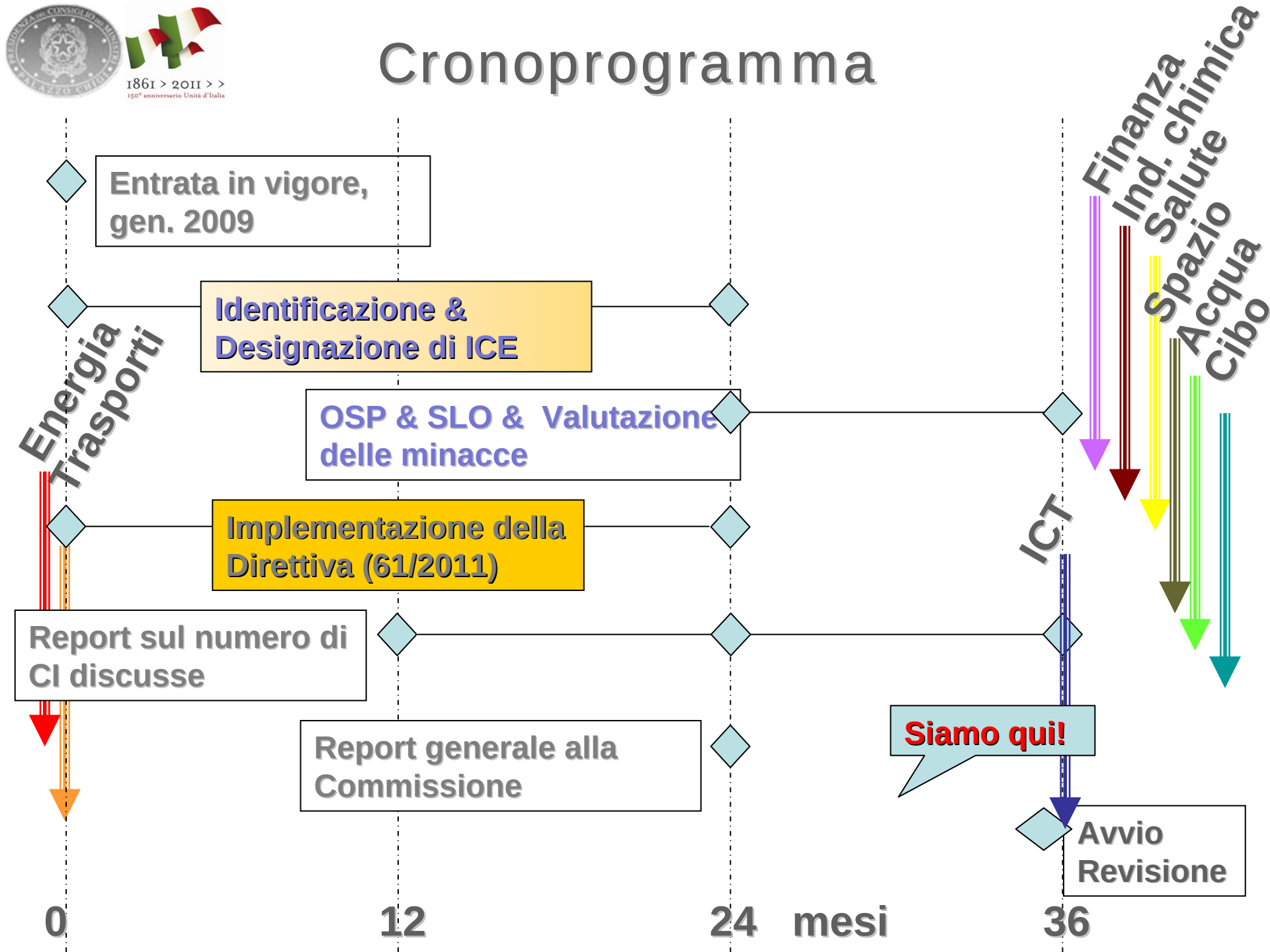
- Casualties
- Economic losses and impacts
- Economic security
- Physical suffering
- Disruption to daily life
- Public confidence
- Public health and safety
- Psychological impacts
- National security impacts
- Impact on Government's services
- Territory infringement
- Public outrage and fear
- Violation of democracy
- Impact on social order
- Geopolitical impact
- National morale
- Environmental impacts
- Sociopolitical impacts
- Detrimental effects on brand-value

Time and space (zone of interest)

Loss of service Quality of Good/Service (of Infrastructures)



Cronoprogramma



Infrastrutture critiche (IC)

Nel 2006 è stato costituito, presso l'Ufficio del Consigliere Militare, il Tavolo interministeriale di coordinamento per la protezione delle Infrastrutture critiche (tavolo PIC) che:

- **ha definito, di volta in volta, la posizione nazionale in merito alle iniziative ed attività in ambito UE o di altri consessi internazionali;**
- **ha avuto l'obiettivo di stabilire le procedure per la individuazione e designazione delle IC nazionali;**
- **ha dato mandato alla Commis. Intermin. Tecnica di Difesa Civile (CITDC) di elaborare i criteri per l'individuazione delle IC nazionali**

Infrastrutture critiche (IC)

Commissione Interministeriale Tecnica di Difesa Civile (CITDC)

costituita ad ott. 2001 per supportare l'organizzazione nazionale di gestione delle crisi

Ha elaborato, in coordinamento con l'Ufficio del Consigliere Militare, le procedure per l'individuazione e designazione delle Infrastrutture critiche nazionali (ICN)

Infrastrutture critiche (IC) e loro protezione

Infrastrutture Critiche Europee (ICE)

Direttiva Europea n. 114 / 2008

settori Energia e Trasporti

designazione individuazione e protezione minima

recepimento
entro 12 gennaio 2011

Come previsto dalla Legge comunitaria 2009, è stato approntato un D. Lgs. approvato l'11 gennaio 2011 dal Consiglio dei Ministri e il 21 febbraio dalle Camere

Decreto legislativo

Il Decreto Legislativo affida al Nucleo interministeriale situazione e pianificazione (NISP), istituito con decreto del Presidente del Consiglio dei Ministri 25 maggio 2010, le funzioni specificate nel D. Lgs. per l'individuazione e la designazione delle ICE

Per tali fini il NISP è integrato dai rappresentanti del Ministero dello sviluppo economico, per il settore energia, del Ministero delle infrastrutture e dei trasporti ed enti vigilati, per il settore trasporti

Decreto legislativo

Il Decreto Legislativo individua una ‘struttura responsabile’, cui sono affidate, per il supporto al NISP, le attività tecniche e scientifiche riguardanti l’individuazione delle ICE e per ogni altra attività connessa, nonché per i rapporti con la Commissione europea e con le analoghe strutture degli altri Stati membri dell’Unione europea

Segreteria IC

Il DPCM di organizzazione dell'Ufficio del Consigliere Militare della Presidenza del Consiglio dei Ministri del 22 dicembre 2010 istituisce la Segreteria per le infrastrutture critiche (SIC) presso il medesimo Ufficio.

La Segreteria cura il coordinamento interministeriale delle attività nazionali, anche in ambito internazionale, e delle attività tecniche e scientifiche per l'individuazione e la designazione delle infrastrutture critiche nazionali ed europee e concorre al coordinamento per la loro protezione.

Decreto legislativo

Il ministero delle infrastrutture e trasporti e il ministero dello sviluppo economico individuano le possibili ICE

La SIC, insieme al Ministero degli affari esteri, dell'interno e della difesa, e al Dipartimento della protezione civile effettuano le negoziazioni con gli Stati Membri interessati

Il NISP, integrato dal ministero delle infrastrutture e trasporti e dal ministero dello sviluppo economico designa le ICE su territorio italiano

I settori nel decreto legislativo per le ICE

Settore **ENERGIA**
Sottosettori:
- **Elettricità**, comprendente: infrastrutture e impianti per la produzione e la trasmissione di energia elettrica e per la fornitura di elettricità;
- **Petrolio,** comprendente: produzione, raffinazione, trattamento, stoccaggio e trasporto di petrolio attraverso oleodotti;
- **Gas,** comprendente: produzione, raffinazione, trattamento, stoccaggio e trasporto di gas attraverso oleodotti e terminali GNL;

Settore **TRASPORTI**
Sottosettori:
- **Trasporto stradale;**
- **Trasporto ferroviario;**
- **Trasporto aereo;**
- **Vie di navigazione interna;**
- **Trasporto oceanico, trasporto marittimo a corto raggio e porti.**

I criteri nel decreto legislativo per le ICE

CRITERI SETTORIALI

Sono riportati nelle linee guida emesse dalla Commissione Europea, sono riservati.
Le soglie vengono stabilite caso per caso dalla SIC con i Ministri competenti a livello settoriale.

CRITERI INTER SETTORIALI

Effetti negativi

1. le possibili vittime, in termini di numero di morti e di feriti;
2. le possibili conseguenze economiche, in termini di perdite finanziarie, di deterioramento del bene o servizio e di effetti ambientali;
3. le possibili conseguenze per la popolazione, in termini di fiducia nelle istituzioni, di sofferenze fisiche e di perturbazione della vita quotidiana, considerando anche la perdita di servizi essenziali.

Soglie

La SIC effettua discussioni bilaterali o multilaterali con gli altri Stati Membri coinvolti dalla IC sotto esame e preliminarmente, in tali discussioni, fissa, in accordo con gli altri Stati, limiti comuni dei criteri di valutazione intersettoriale.

Osservazioni generali

La direttiva europea basa l'analisi della "criticità" sulla valutazione di impatto e non sulla analisi del rischio: in tal modo non occorre verificare le vulnerabilità dell'operatore in fase istruttoria (verifica che non trova il favore degli operatori); inoltre la valutazione di impatto prescinde dalla minaccia che origina l'evento.

La valutazione di impatto indicata dalla direttiva si basa sulla valutazione del degrado della qualità del servizio/bene resa ai cittadini. Si valuta la qualità "a regime" e si calcola l'effetto del suo degrado parziale o totale. L'effetto si misura con i criteri intersettoriali.

Non esiste in letteratura un metodo consolidato per effettuare l'analisi di impatto come definita nella direttiva europea (né la direttiva affronta tale problema).

Fondazione Ugo Bordoni FORMIT THEOREMATICA®

Il progetto DOMINO è realizzato in cooperazione con:

- *Presidenza del Consiglio dei Ministri - Italia*
- *Home Office - Regno Unito*
- *SGDN Sécrétariat General de la Defense Nationale - Francia*
- *Ministry of Emergency Situations - Bulgaria*

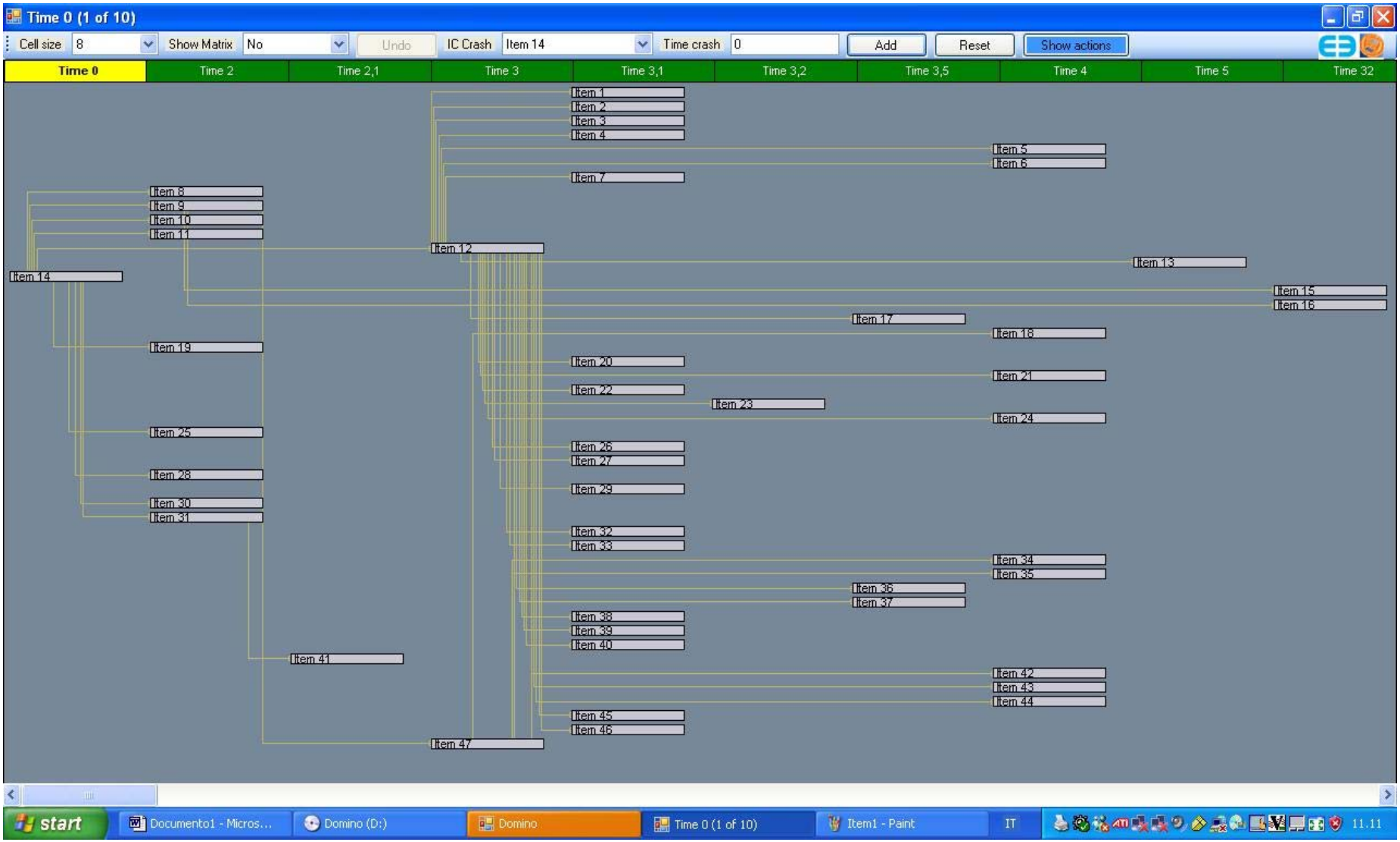
Domino effect modelling infrastructures collapse

Indagine Pilota

v. 5, 8 luglio 2010

With financial support from the Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks Programme
European Commission – Directorate-General Justice, Freedom and Security

Esempio di output del progetto DOMINO



Internet resilience and stability

Non-paper on the European principles and guidelines for Internet resilience and stability

Version 3.0 dated 12/10/2010
Following Communication COM(2006) 251 on a Strategy for a Secure Information Society

The Internet
For the purposes of interpreting and applying the principles for Internet resilience and stability ("the Principles"), the Internet is to be understood as the global and public network of networks whose nodes communicate with one another using the TCP/IP family of protocols and are identified by a globally unique address assigned

Internet resilience and stability

Preamble

- The Internet
- Coherence with Core European values and Interests
- The Global Context
- International Cooperation

I. A Matter of Public Policy

- Role of Public Authorities
- Importance of a Multi-stakeholder Approach
- Importance of incentives

II. A necessary well-functioning market

- Strengthening the European ICT security industry
- Good Risk Management
- Openness and Interoperability
- Open Standards

III. Cooperation

- Cooperation and Mutual Assistance
- Tools and Instruments
- Education and Awareness-Raising

Internet resilience and stability

Importance of incentives

To pursue the objective of ensuring the stability and resilience of the Internet, public authorities should, as appropriate, give balance between soft and hard regulation taking into account the extremely dynamic nature of the Internet and its crossborder and global nature Soft regulation could include the application of appropriate social and economic incentives that could achieve this goal. Coordination of policies at the EU level will avoid fragmentation of the internal market.

Non-paper on ICT criteria

Identified types of infrastructure for voice communications with cross-border dimension

- **Types of infrastructure for voice communications:**
  - Main cross-border sea and land cable routes and nodes
  - International switching gateways/centres
  - Devices enabling international roaming
  - Home Location Registers (HLR) which comprise data of subscribers from Member State different from the Member State where the HLR is located
  - Network Operation Centres (NOC) for management of the aforementioned services and infrastructures

Non-paper on ICT criteria

Identified types of infrastructure for data communications with cross-border dimension

- **Types of infrastructure for data communications:**
  - Main cross-border sea and land cable routes and nodes
  - Cable routes of domestic physical networks the loss of which would have an impact on other Member States (single points of failure)
  - Internet Exchange Points (IXPs) and large private peering points
  - European root DNS servers
  - DNS servers for .eu
  - Dedicated routers (e.g. in MPLS core networks)
  - Dedicated time servers
  - Network Operation Centres (NOC) for management of the aforementioned services and infrastructures
  - RIPE database (containing registration information for networks in the RIPE NCC service region and related contact details)

Non-paper on ICT criteria

Identified types of infrastructure for data storage and data processing with cross-border dimension

- **Types of infrastructure for data storage and specific data processing:**
  - Dedicated data centres
  - Backup centres (computer resilience centres)
  - Content Delivery Networks (CDN)/ Centres
  - Dedicated time servers

Non-paper on ICT criteria
Overview on ICT criteria

Specific criteria:

1. **Cross-border cable routes and nodes** criterion
2. **IXP and peering point** criterion
3. **Root DNS server** criterion
4. **Router** criterion
5. **Time server** criterion

General criteria:

6. **Telecommunications equipment** criterion
7. **TLD .eu infrastructure** criterion
8. **Internet registration** criterion
9. **Data centre** criterion
10. **Single points of failure on request** criterion
11. **Communications default** criterion
12. **Important Internet infrastructure** criterion

Non-paper on ICT criteria

Proposed ICT criteria – one example

- **Cross-border cable routes and nodes criterion:**
  A cross-border cable route between two Member States (including its trunks, its end nodes and all nodes in between as well as the corresponding management facilities) the capacity of which accounts for more than x % of the cross-border capacity of each of at least two Member States and the disruption or destruction of which could not be compensated within n hours.

EP3R and EFMS

ESTABLISHMENT OF A
EUROPEAN PUBLIC-PRIVATE PARTNERSHIP FOR RESILIENCE
(EP3R) 2010

In the initial running phase, it is proposed that EP3R **prioritises the resilience challenges within the ICT sector**.
EP3R is **complementary to the European Forum for Member States (EFMS)**. EFMS is a platform dedicated to national public authorities to share information and good policy practices as well as to conduct policy discussions on security and resilience of CIIs. While EFMS is dedicated to Member States' public authorities, EP3R will serve as an exchange and partnership platform for the public and private sector.

US International Strategy for cyberspace, may 2011

The same global networks that power innovation also open up new avenues for industrial espionage and the theft of intellectual property and commercial information. **Cyberspace can be used to steal an unprecedented volume of information from businesses, universities, and government agencies**; such stolen information and technology can equal billions of dollars of lost value. Individual incidents often go unreported.

The United States will take measures to identify and respond to such actions to help **build an international environment that recognizes such acts as unlawful and impermissible, and hold such actors accountable**

Direttiva 140/09

DIRETTIVA 2009/140/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 25 novembre 2009
recante modifica delle direttive 2002/21/CE che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, 2002/19/CE relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime e 2002/20/CE relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica

Direttiva 140/09

Articolo 13 bis
Sicurezza e integrità
Gli Stati membri assicurano che le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico **adottino adeguate misure di natura tecnica e organizzativa per gestire adeguatamente i rischi per la sicurezza delle reti e dei servizi**. Tenuto conto delle attuali conoscenze in materia, dette misure assicurano un livello di sicurezza adeguato al rischio esistente. In particolare, si adottano misure per **prevenire e limitare le conseguenze per gli utenti e le reti interconnesse** degli incidenti che pregiudicano la sicurezza.
Gli Stati membri assicurano che le imprese che forniscono reti pubbliche di comunicazioni adottino tutte le misure opportune per garantire l'integrità delle loro reti e **garantire in tal modo la continuità della fornitura dei servizi su tali reti**.

Directive proposal on cyber attacks

Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, presented by justice DG

Criminal offences:
Illegal access to information systems
Illegal system interference
Illegal data interference
Illegal interception
Tools used for committing offences
Incitement, aiding and abetting and attempt

punishable by effective, proportionate and dissuasive criminal penalties (2 to 5 years of prison).

EU INITIATIVES ON CYBER SECURITY

- Ministerial Conference on Critical Information Infrastructure Protection (Balatonfured 14 – 15 April 2011) stated that Member States shall intensify their efforts in reinforcing their national cyber-security capabilities and in driving forward the European cooperation as a step towards reinforced International cooperation
- The last EU Council of Ministers confirmed the Ministerial Conference conclusions

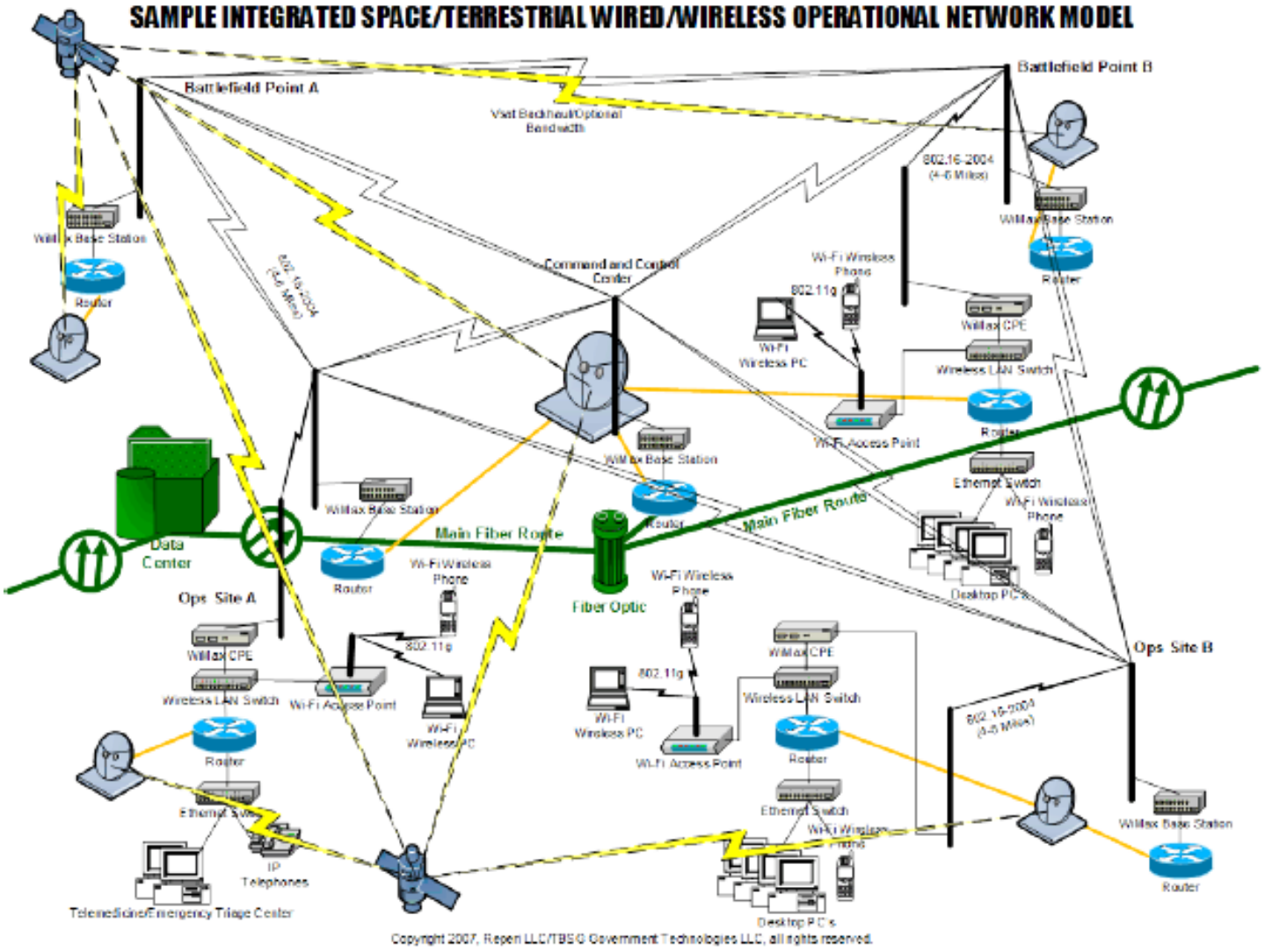
BALATONFURED CONCLUSIONS

- Adoption of National Cyber-Security strategy
- Establishment of National / Governmental CERTs
- Creation of a network of CERTs at European level
- Definition of Cyber incidents contingency plan
- Participation to the ENISA's activities
- Organisation of National Exercise and participation to second pan-european exercise
- Development principles for the stability and resilience of Internet
- Participation to the activities of the EU − US working group
- Support to development of international cooperation mechanisms

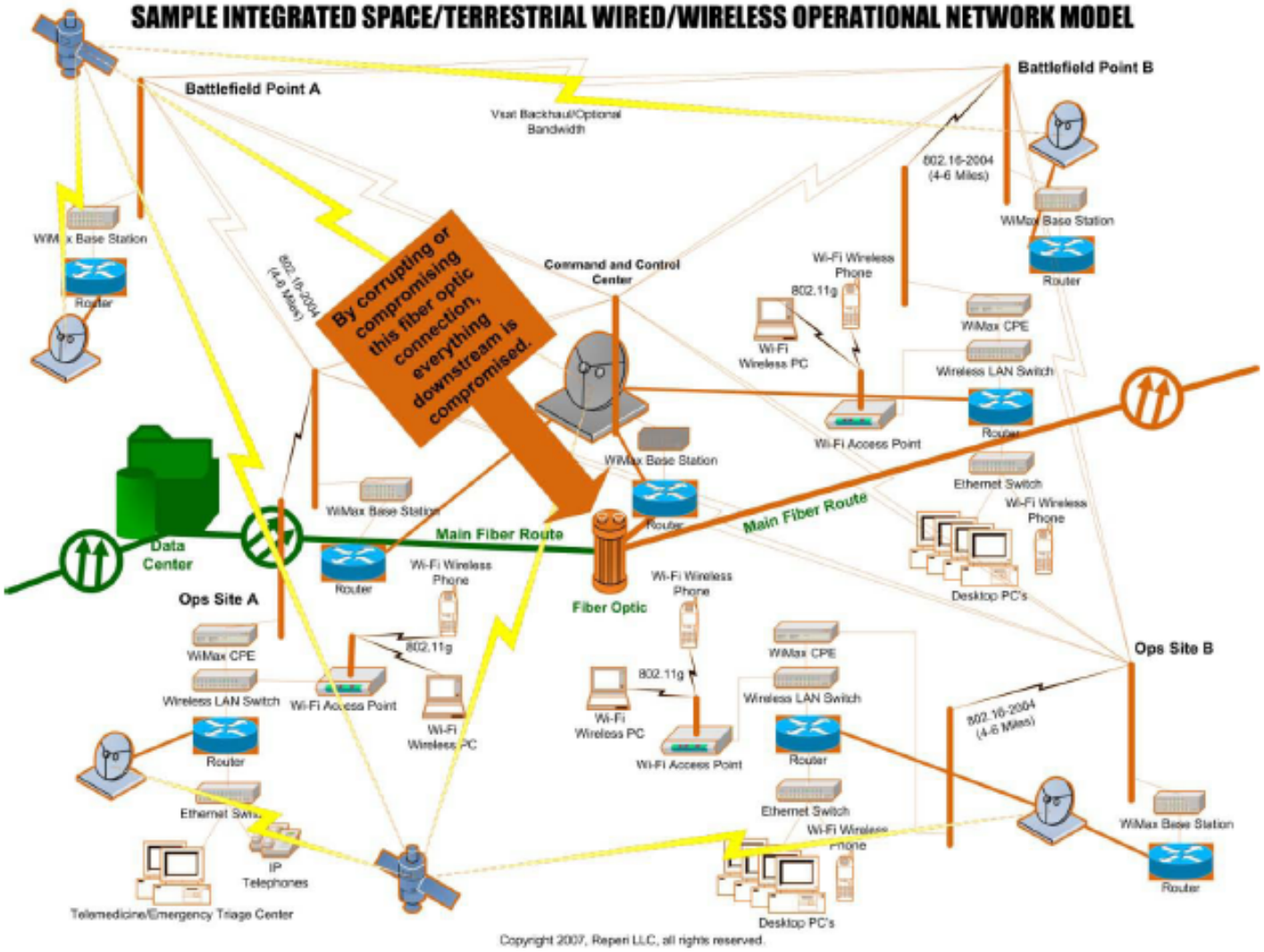
Le linee di carrier

Source: Global Crossing, "Carrier Overview," 2010.

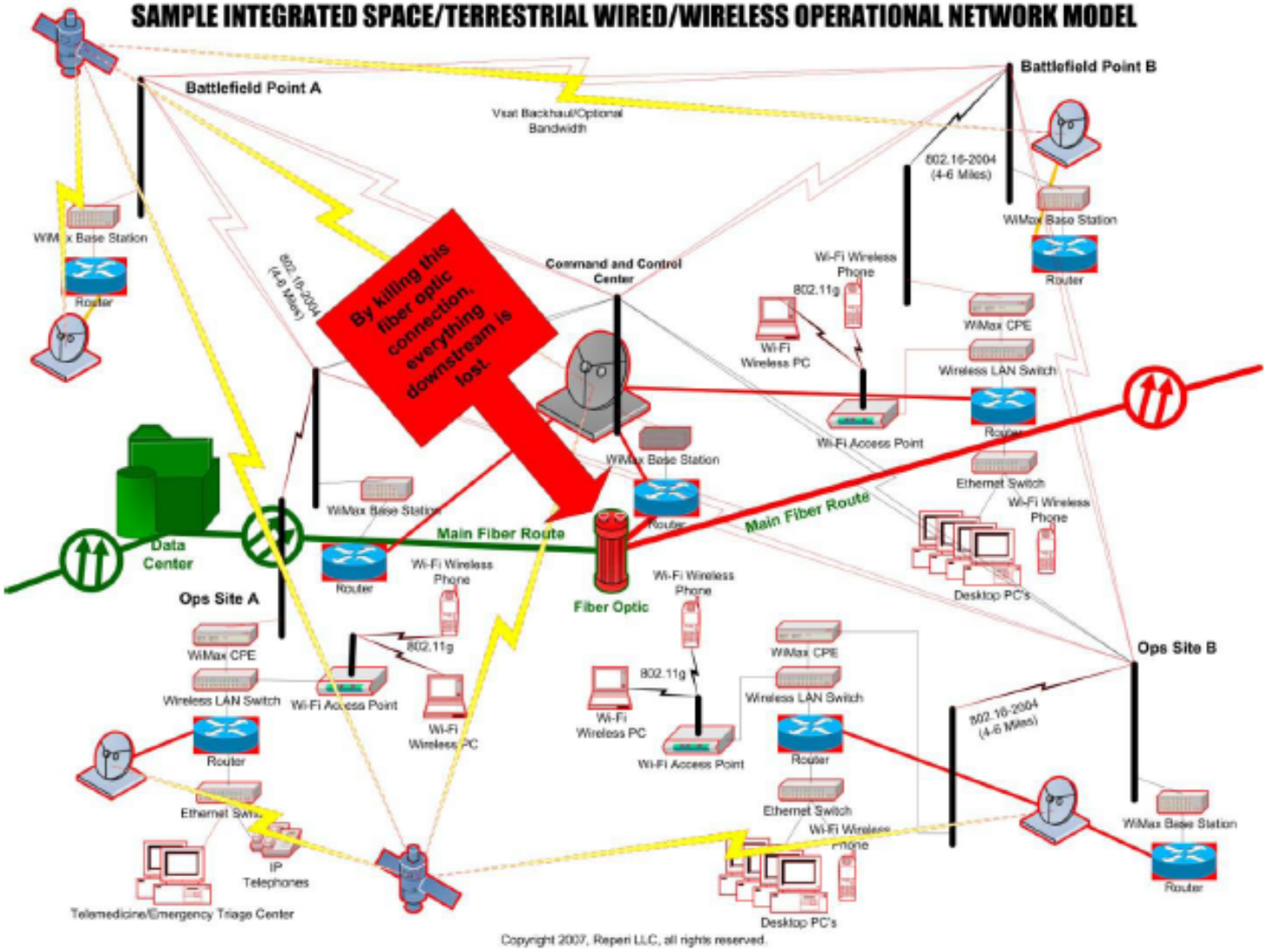
TLC system example

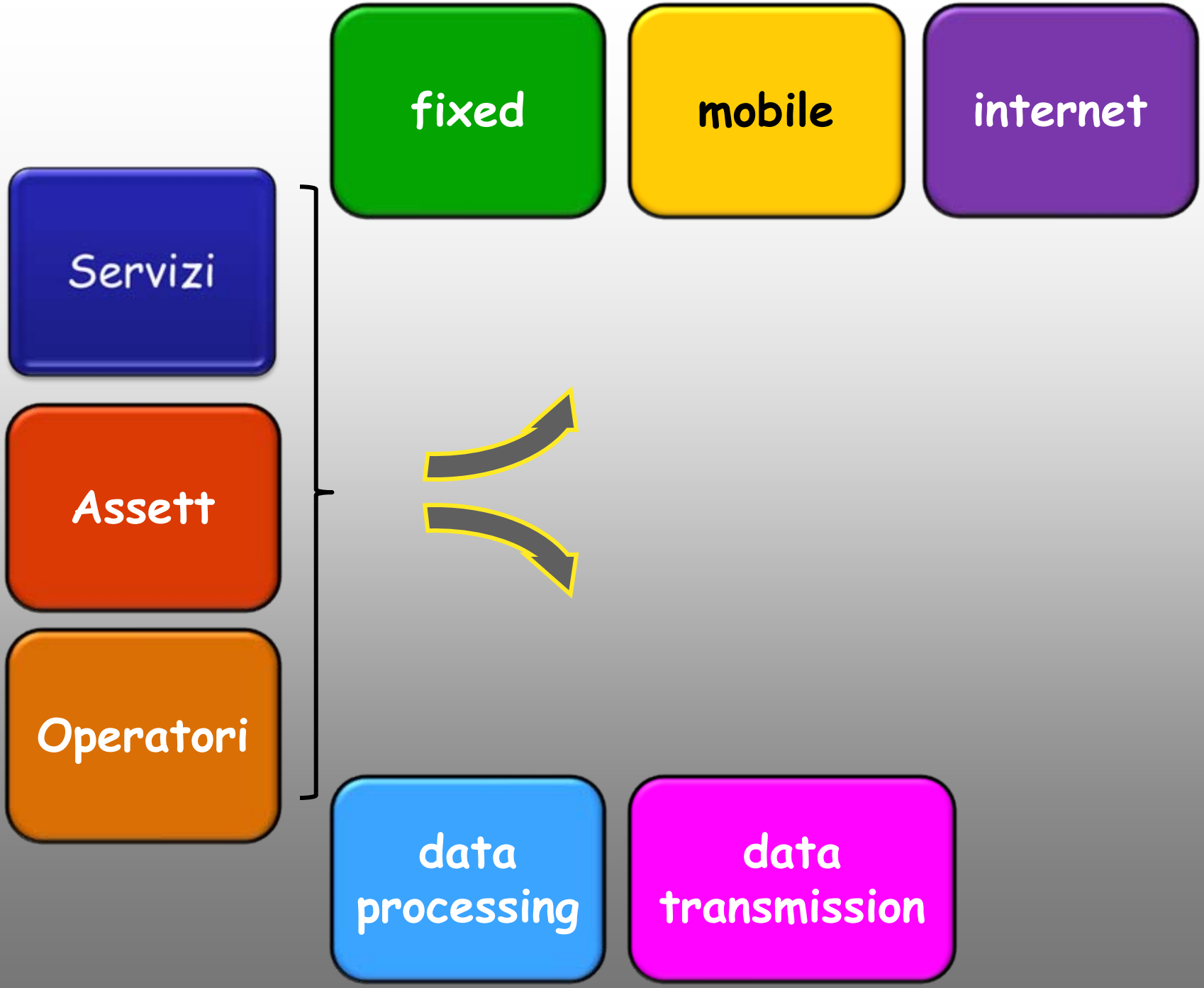


Vulnerabilities



Vulnerabilities

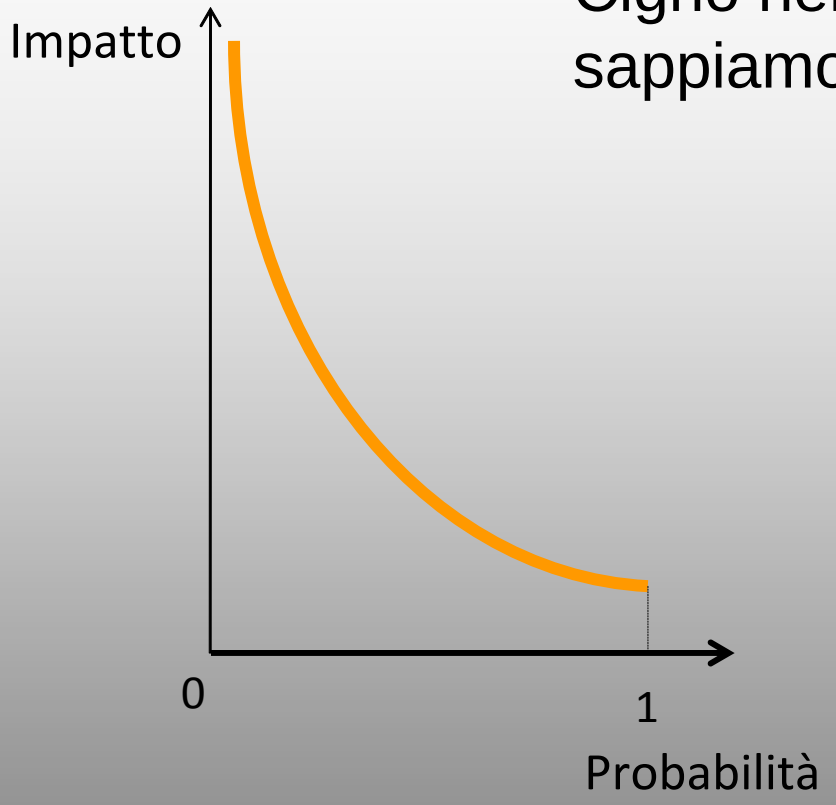



fixed
mobile
internet
Servizi
Assett
Operatori
data processing
data transmission

Il cigno nero

Nassim Nicholas Taleb

Cigno nero: Evento non noto, non ne sappiamo calcolare alcuna caratteristica



- Eventi antropici
- Clima spaziale
- Premonizioni e millantate previsioni

PRESENTATION

- 10 MARCH. ARTICLE NEW YORK TIMES
EXCESSIVE COVERAGE BY PRESS
PUBLIC OPINION CONCERNED

- 23 MARCH. SPANISH AUTHORITIES ORGANISED A THREE-DAY-LONG SEMINAR ON SPACE WEATHER.

- 11 APRIL. CNPIC TOOK PART IN THE SECOND ELECTRICITY INFRASTRUCTURE SECURITY SUMMIT, WHICH WAS HELD IN WASHINGTON D.C., AND SUPPORTS THE ROADMAP FOR INTERNATIONAL COOPERATION THAT WAS PROPOSED IN IT.

IMPACT OF SOLAR STORMS ON EARTH

3 KINDS OF PHENOMENA:

- ✓ SOLAR FLARES
- ✓ CORONAL MASS EJECTIONS
- ✓ SUNSPOTS

ENISA Exercise

1st pan-European cyber security exercise **"CYBER EUROPE 2010“** which was successfully conducted on 4th of November 2010.

- **Thirty European countries (all 27 EU Member States plus Iceland, Norway and Switzerland)** were involved in the organisation and running of the exercise which was supported by ENISA and the European Commission's Joint Research Centre.
- The main objectives of the exercise were to build trust and to increase understanding of how management of incidents is conducted in different countries across Europe. The measures **tested** were **the functioning of contact points in the countries involved, communication channels and the types of data that would be exchanged over those channels as well as the understanding of each others mandate and decision-making power**.

Cyber storm

Preliminary results from Cyberstorm III conducted in September 2010.

• The **Cyber Storm exercise series,** which is sponsored by the U.S. Department of Homeland Security (DHS), aims to improve the capabilities of the cyber incident response community, encourage the advancement of public-private partnerships

• More specifically, the very first objective of Cyberstorm III was to exercise the **National Cyber Incident Response Plan (NCIRP)** developed by DHS in response to the Cyberspace Policy Review.

• Cyberstorm III also included testing effective operation of the **National Cybersecurity and Communications Integration Center (NCCIC)** inaugurated in October 2009. NCCIC is a 24-hour, DHS-led watch and warning centre addressing threats and incidents affecting the nation's cyber infrastructure.

• Cyberstorm III consisted in **three full days of live exercise**, from 28th to 30th of September 2010, played by more than 1700 participants, combining private sector and government (70 private sector organisations).

The “Cyber Shot 2010”

- National Cyber Defense Exercise
- Contemporaneous to the NATO “Cyber Coalition 2010”
- Military and Civilian Agencies involved
- Multilevel involvment
- This exercise live and paperless (as much as possible)
- National Industry contribution and support

G8

1. protection of intellectual property, in particular copyright

2. protection of personal data and people's privacy on the Internet

3. *security of the Internet* is a multi-stakeholder

4. universal access to the Internet for developing countries

5. multi-stakeholder model of Internet governance. Among them, flexibility and transparency have to be maintained

Economics of security

Ovierview of the main topics

1. **Economic impact in case of CI disruptions**
   - Direct effects (instantaneous effects) of malicious attacks and/or critical events (private perspective)
   - Indirect effects (cascading effects) of malicious attacks and or critical events (social perspective)
2. **Costs/benefits of security and resilience (investments)**
   - Mainly ex-ante private costs
   - Mainly social costs for indirect effects
3. **Incentives to reduce market failures and negative externalities**
   - From public to private

2. Costs/benefits of security and resilience

Cyber-security focus

The study realizied by **ISCOM in 2006** aims at presenting results of the analysis of a cyber-security breach due to a virus in an Italian medium size enterprise.

Type of costs	Effect
Direct costs	• Loss of production/productivity for the unavailability of ICT • Loss of production/productivity for the restoring of the production • Damages to the assets
Indirect costs	• Emergency management • Consumption of phisical resources
Other costs	• Administrative sanction s • Reputation loss • Damages to the users

2. Costs/benefits of security and resilience

Cyber-security focus

Scenario 1 – Software and training investments of a medium-size enterprise in the **health sector**

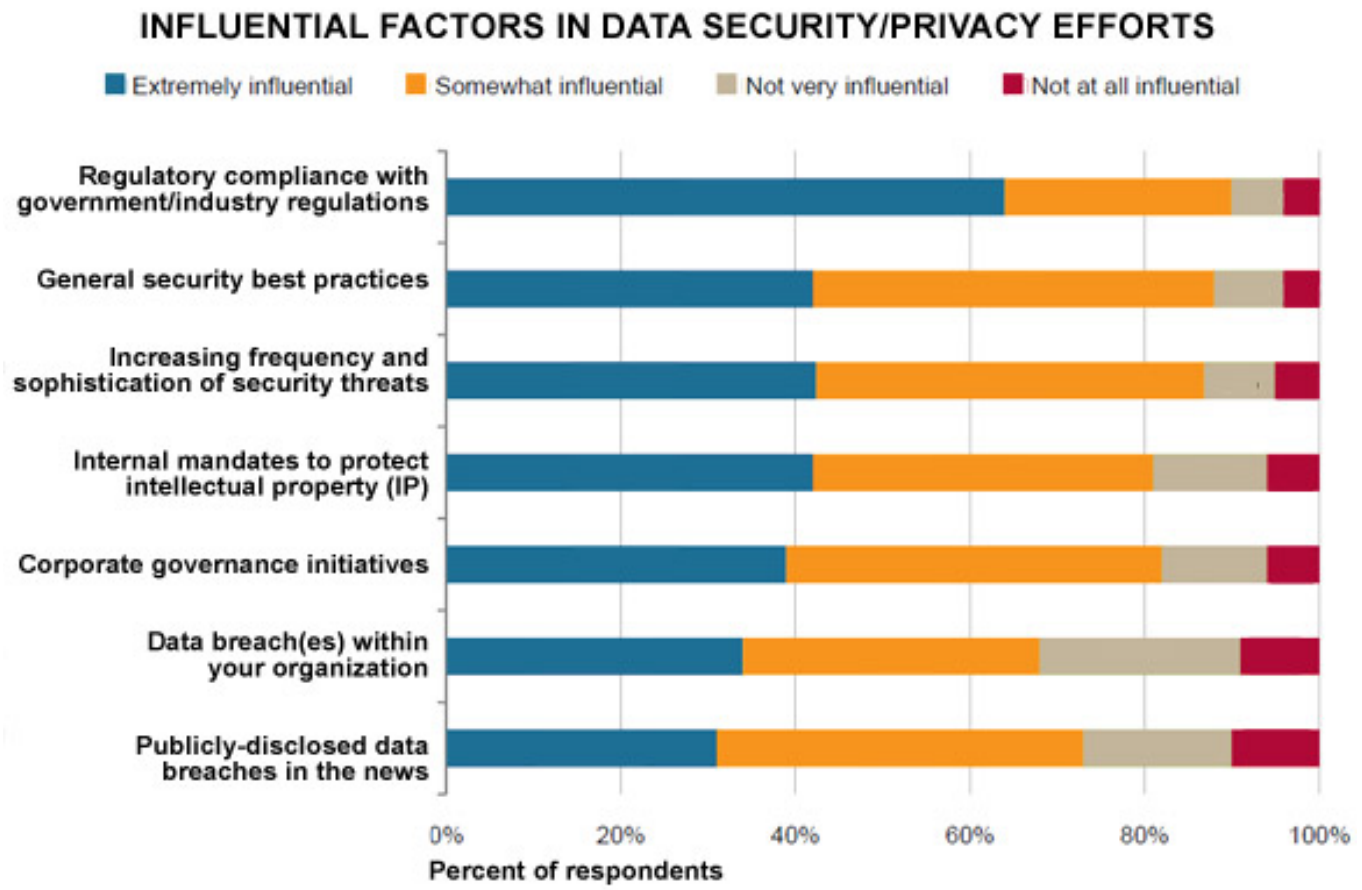
NON SECURITY COSTS	**€ 191.000**
SECURITY COSTS	**€ 54.000**
SAVING	**€ 137.000**
SAVING (%)	**72 %**

Scenario 2 – Software and training investments of a medium-size enterprise in the **ICT sector**

NON SECURITY COSTS	**€ 75.000**
SECURITY COSTS	**€ 40.000**
SAVING	**€ 35.000**
SAVING (%)	**47 %**

3. Incentives

Alternative to regulation



Keeping up: The Enterprise Strategy Group, a consulting firm, asked 308 IT professionals in large companies what factors motivated their decisions to improve data security. Regulatory compliance topped the list .
Credit: Credit: *ESG Research Report, Protecting Confidential Data Revisited, April 2009*

Economics of security
Topics recently investigated

- **Annual WEIS conference The Tenth Workshop on Economics of Information Security (WEIS 2011, June 14–15)**
  http://weis2011.econinfosec.org/

- Attacks effects and their pervasiveness
- Identity theft and privacy issues
- Resilience of systems
- Investment rigidities
- Liability policies
- Demand for security
- Security standardization

Presidenza del Consiglio dei Ministri

l.franchina@governo.it