The Directive on European Critical Infrastructure Protection

Mike Thornton

IPSC - Institute for the Protection and Security of the Citizen
Ispra - Italy

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/
The security and economy of the EU, as well as the well-being of its citizens, depends on certain infrastructures and the services they provide.

The destruction or disruption of key infrastructures could entail the loss of lives and property, as well as a collapse in public confidence.
Following the atrocities of 11 September 2001 in New York and the Madrid train bombing in 2004, the European Council asked the European Commission to prepare an overall strategy to protect critical infrastructure within the EU.

On December 2006, the Commission proposed a directive to Council regarding the identification and designation of European Critical Infrastructure (ECI).

European Programme for Critical Infrastructure Protection (EPCIP)
While recognising the threat from terrorism as a priority, we must also recognise that naturally occurring events or accidents can have the same effect (disruption or destruction of infrastructure).

The protection of critical infrastructure will be based on an all-hazards approach.

The first challenge is to identify European Critical Infrastructure (ECI).

*Then ensure it is adequately protected*
Critical Infrastructure Event Cycle

ID & Designation → Protection → Indication & warning → Mitigation → Response → Reconstruction

Pre-Event → Event → Post-Event
As it is impossible to protect all infrastructure in Europe

We must protect the most critical

How can we identify what is European Critical Infrastructure?
The identification phase is the foundation and most important phase of the CIP life cycle.

This phase identifies the assets absolutely critical to Europe and determines the assets’ vulnerabilities, as well as their interdependencies, configurations, and characteristics.
DHS asked the States to identify assets they considered critical
National Asset Database Entries by Sector

77,069 assets

- Dams, 2029
- Telecommunications, 3020
- Information Technology, 757
- Water, 3842
- Banking & Finance, 669
- Transportation, 6141
- Postal & Shipping, 417
- Agriculture & Food, 7542
- Not Specified, 290
- Energy, 7889
- Emergency Services, 2420
- Chemical & Hazardous Materials, 2963
- Commercial Assets, 17327
- Defense Industrial Base, 140
- Government Facilities, 12019
- Nuclear Power Plants, 178
- Public Health, 8402
- National Monuments & Icons, 224

Critical Infrastructure: The National Asset Database 16 July 2007 RL 33648
Dept. of Homeland Security had to screen and analyse the 77,069 assets (based on criteria)

Identified ~2,500 assets that it considered to be critical to the nation

Based on its analysis of vulnerability to attack or natural events and the possible consequences
Let the Member States decide what is critical

Based on agreed procedure containing selection criteria

Member States will notify the Commission of the critical infrastructures which satisfy the pre-established criteria
The Directive includes a common procedure for the identification and designation of European Critical Infrastructures (ECI)

A 4 step process

1. Are the Sectorial Criteria met?
2. Is the Infrastructure critical?
3. Is there a trans-boundary impact?
4. Are the Cross-Cutting criteria met?

If accepted by the relevant MS, the CI is designated as an ECI
“Gas transmission pipelines that ensure a capacity of at least X million normalized m$^3$/h at a transit-border point”
Sectors to be used for the purposes of implementing the Directive; energy and transport
Subsequent sectors to be used for the purpose of implementing this Directive may be identified

Priority should be given to the Information and Communication Technology (ICT) sector
Sub-sectors

1. Electricity
Infrastructures and facilities for generation and transmission of electricity in respect of supply of electricity

2. Oil
Oil production, refining, treatment, storage and transmission by pipelines

3. Gas
Gas production, refining, treatment, storage and transmission and distribution by pipelines
LNG terminals
ECI sectors: Sector II Transport

Sub-sectors

4. Road transport
5. Rail transport
6. Air transport
7. Inland waterways transport
8. Ocean and short-sea shipping and ports
Step 2: Is the Infrastructure critical?

Does it satisfy the definition of Critical Infrastructure?

“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;
Is it a National Critical Infrastructure?

If in all Member States, their National Critical Infrastructure are protected – probably no need for this directive

It is unlikely that that an ECI is not a national CI

But it could be possible
Step 3: Is there a trans-boundary impact?

Does it satisfy the definition of European Critical Infrastructure?

“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;
Step 3: Is there a trans-boundary impact?

“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.
Previous implementations of similar programmes, e.g. in Canada, Australia or the US have been applied to single countries and not to a group of countries.

Already exists national CI protection programmes

Complement these EPCIP works in a trans-boundary context
A national problem, not to be considered as potential ECI.

The biggest fire in Europe since World War Two.
“We weren't very far from a European blackout“
spokesperson from RTE (French transmission system operator)

Caused a European problem, a potential ECI
380kV lines across river Ems turned off at 21:30h to let the Norwegian Pearl through

Other lines take the load

Overloaded line Landesbergen Wehrendorf trips

Other lines trip in an unstoppable cascade within seconds of each other

First 14 lines tripped within 14 s

Total 33 lines tripped within 1 min 20s
A large number of lines in Germany, Austria, Hungary and Croatia automatically tripped one after the other in a "domino" effect, as their automated protection systems detected load flows over the safety limit.

Then France, Belgium, Italy, Spain, Portugal, Slovenia and the Netherlands.

European grid is split into three, frequencies drift apart and there was a shortage of generating capacity in the West.

15 million households affected in 11 countries.

Power restored in 30 minutes in some places, 2 hours in Italy.
Step 4: Cross-Cutting Criteria

Cross Cutting Criteria

- Energy
- Transport
- ICT
- Water
- Food
- Health
- Financial
- Chemical industry
- Space
The cross-cutting criteria are developed on the basis of severity of impact of the disruption or destruction of the CI.

The severity of impact should be assessed on the basis of.
Severity of the impact

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

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

*Public effects criterion* (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including potential environmental effects including the loss of essential services).
Atocha station Madrid
13 Improvised Explosive Devices (IEDs) on 4 trains
1\textsuperscript{st} train 3 IEDs exploded 07:37 at Atocha
2\textsuperscript{nd} train 2 minutes late ~500m from Atocha 4 IEDs exploded 07:39
3 other IEDs found unexploded on train
Had the second train been on schedule and the three other devices detonated properly it is believed that the effect would have caused catastrophic damage to the station possibly collapsing the roof and increasing the death toll
11,400,000 demonstrators (28% of Spanish population)
Potential infrastructure under investigation

Experts identify the worst possible realistic scenarios of disruption or destruction of that infrastructure (all hazards, ex-ante exercise)

Each scenario is developed (including cascading effects where possible) and its impact assessed in terms of the 3 dimensions (casualties, economic and public effects)

Apply CCC to each scenario until one is met
Ex-ante analysis
Use reasonable worst case scenarios
Terrorist attacks are becoming more sophisticated, better targeted and often consist of multiple independent attacks
7 July 2005

1. 8:51 a.m. Explosion in Tunnel between Aldgate and Liverpool (7 Dead)
2. 8:56 a.m. Explosion in Tunnel between King's Cross and Russell Square (21 Dead)
3. 9:17 a.m. Train explosion close to Edgware Road station (7 Dead)
4. 9:47 a.m. Bus explosion at Tavistock Square (13 Dead)
A vulnerability analysis of the London underground network suggests that the stations bombed on 7 July, 2005 may not have been chosen randomly.

From the viewpoint of effectively disturbing the transport system, nearly the best choice was made out of roughly 3 million possible combinations for attacking three stations.
1. Casualties

2. Economic effects

3. Public effects

4. (Environmental effects)
Estimate the number of casualties (deaths, with no time limit and or seriously injured) due to the destruction or disruption of an infrastructure.

Incidental casualties not counted (depends on modus operandi).

Compare to a threshold.
Estimate the Economic Loss caused by a destruction or disruption of infrastructure
Do not include incidental costs (emergency response services, police, fire service etc)
Do not include repair costs (dependent on modus operandi)
Count costs related to loss of service (until re-instated)
Consider alternatives
Use Best Practices to assess cascading effects

Compare to a threshold
Alternatives and cascades

This calculation should take into account whether alternatives or temporary solutions may be found

Including the additional costs these incur

Cascading effects should be counted where it can be demonstrated that it can be reasonably calculated
Mont Blanc fire 24 March 1999

- 40 dead, 34 injured
- Refurbishment 300 million euros
- Tunnel closed for nearly 3 years
- Alternative Fréjus tunnel
- Loss to Italian economy 1.75 billion euros
When does an effect in terms of economic loss start to become significant in a country?

Assess on a case-by-case basis
The Public effect criteria shall capture the impact on society following the disruption or destruction of an ECI. No direct ways of quantifying Public Effects is known. A qualitative approach must be taken.
Public effects are expressed in 3 categories

1. Physical suffering
2. Disruption to daily life
3. Public confidence

These categories will be assessed in terms of
1. Number of people impacted
2. Severity of the impact
Physical suffering

Lack of drinking water
Lack of food
Lack of shelter
Lack of warmth
Lack of proper sanitary conditions
Health effects
Etc. etc...
Disruption to daily life

Loss of physical security
Loss of income/employment
Displacement from family/social network
Loss of purchasing power
Loss of quality of living space
No access to information resources
Increase in commuting time
Decrease in comfort
etc. etc.....
Public confidence

Violation of public order, looting, panic, stocking up
Ex-Ante Assessment

Estimate the number of people impacted;
Severity refers to the magnitude of the impact;

We distinguish three levels of increasing severity:

1. Inconvenient
2. Disruptive
3. Dysfunctional

Partially Based on EURAM (European risk assessment methodology) which identifies three levels of psychological severity
1. **Inconvenient:** irritating for the individual, but not disruptive for his/her daily routine

   AZ1050  Milan Malpensa  21.45  Delayed 23.10

2. **Disruptive:** the individual will have to adapt his/her daily routine

   AZ1050  Milan Malpensa  21.45  Cancelled

3. **Dysfunctional:** the individual is no longer able to continue his/her daily routine

   - - - - -  All Flights  Cancelled until further notice
For each of the 3 categories

1. Physical suffering
2. Disruption to daily life
3. Public confidence

Assess and score in a matrix, compare to a threshold
Environmental effects
Only 2 parameters

• Displacement of people
• Unavailability of territory
• Assess these economically and compare to the economic threshold
Designation process

Country where infrastructure resides

Identification and ex-ante assessment of potential ECI

Inform and Identify potential ECI to MS

TIME

Consolidation discussions

IF all agree ECI

Review

Country that may be affected
Following designation

Within 12 months of designation of an ECI

Operator Security Plans or equivalent measures comprising an identification of important assets, a risk assessment and the identification, selection and prioritisation of counter-measures and procedures should be in place in all designated ECI’s
With a view to avoiding unnecessary work and duplication, each MS should first assess whether the owners/operators of designated ECI possess relevant OSP’s or similar measures.

Where such plans do not exist, each MS should take the necessary steps to make sure that appropriate measures are put in place.
Within 12 months of designation of an ECI

Security Liaison Officers should be identified in all designated ECI’s in order to facilitate cooperation and communication with relevant national critical infrastructure protection authorities.

Where such a Security Liaison Officer does not exist, each Member State should take the necessary steps to make sure that appropriate measures are put in place.
Within 12 months of designation of an ECI

Each Member State shall conduct a threat assessment in relation to European Critical Infrastructure sub-sectors within one year following the designation of critical infrastructure on its territory as European Critical Infrastructure within those sub-sectors.
Each Member State shall report every 24 months to the Commission generic data on a summary basis on the types of vulnerabilities, threats and risks encountered per ECI sector in which ECI have been identified.
Timing

This Directive shall be reviewed in three years following its entry into force.

Member States shall take the necessary measures to comply with this Directive at the latest two years after its entry into force.
Where are we now?
Timeline

- 0 Months: Entry into force
- 12 Months: Identification & Designation
- 24 Months: OSP & SLO & Threat Assessment
- 36 Months: Implementation of Directive

Report no. of CI’s discussed

Generic report to Commission

Review
Guideline for implementation

The Commission together with the MS’s shall develop guidelines for the application of the cross-cutting and sectoral criteria and approximate thresholds to be used to identify European Critical Infrastructure.

The criteria shall be classified.

The use of such guidelines will be optional for the MS’s.
The Commission shall support, through the relevant Member State authority, the owners/operators of designated European Critical Infrastructures by:

- **Access to available best practices and methodologies**
- **Support and training**
- **Exchange of information on new technical developments related to critical infrastructure protection**
Sectors to be used for the purposes of implementing the Directive; energy and transport

Subsequent sectors to be used for the purpose of implementing this Directive may be identified

Priority should be given to the Information and Communication Technology (ICT) sector
Nodes on key transmission routes
- Electricity Substations and interconnectors
- Gas Compressor stations
- Oil Ports and pumping stations

- Electricity: High EU criticality due to real-time balancing; inability to store; high societal impacts
- Gas: Major pipelines are critical for electricity generation
- Oil: Limited EU criticality due to flexibility of global market and 90 day storage
The European Energy Supply System is highly interconnected
All 27 EU MS, except Denmark, depend to some extent on imports from neighbouring and non-EU states to meet energy demand
Cyprus (energy dependence rate of 100%), Portugal (99.4%), Luxembourg (99.0%), Latvia (94.0%), Ireland (90.2%)
In total, 56% of the EU’s energy demand is met by imports
Many countries within Europe outsource electrical energy production
France is a large net exporter of electric power while Italy is the largest net importer in Europe, mostly from France, directly or via Switzerland.
More than 80% of Italy’s energy sources are imported
Dependence on electrical transmission system
All night party in Rome

People encouraged to use public transport
Power line which supplied electricity to Italy from Switzerland was damaged by storms, causing it to trip.

Power went off at about 03:20am local time.

Two 400kV power lines between France and Italy tripped due to sudden increased demand.

ENEL lost control of the grid in the next 4s with the lines tripping automatically one by one amid the cascading effect.
Throughout Italy, 110 trains were canceled, with 30,000 people stranded on trains. People could not get home and had to sleep wherever. Police described the scene as chaos but no serious accidents. All flights in Italy were cancelled.
It affected all of Italy, except Sardinia, for 9 hours and part of Switzerland for 3 hours.

It was also the most serious blackout in Italy in 20 years with a total of 56 million people affected.
Russia provides about a quarter of Western Europe's natural gas and most of that - about 80% is shipped through pipelines that cross the Ukraine December 2005 price dispute between Russia and Ukraine.
Russia begun cutting gas supplies to Ukraine on 1 January 2006
Flow reduced into Ukraine by 20%
Russia expected Ukraine to continue pumping all the remaining flow westward
Within hours of Russia disrupting gas supplies a cascading energy emergency moved westward across Europe
Russia accused the Ukraine of withdrawing gas from the export pipelines for its own use
2 January
Hungary was reported to have lost up to 40% of its Russian supplies
Austrian, Slovakian and Romania supplies were said to be down by one third
France 25-30%
Poland by 14%
Italy lost 32 million cubic metres, around 25% of deliveries, during January 1-3
By 4 January Russian gas deliveries to Europe were back to normal levels

No EU country needed to interrupt supplies to customers as a result of the reduction of Russian supplies

Many commercial and industrial customers were not operating over the New Year holiday period
Reflecting the European Union's concern over possible disruption of Russian gas supplies, the E.U. Executive Commission called an emergency meeting of its gas coordination group on January 4 to discuss the issue.

Gas supply seen as critical to Europe
Time is precious in the food chain
Particularly fresh foods
Not cost effective to maintain large stocks,
business wants fast throughput
Food product distribution dependent on transport
The ultimate goal is to run the stores with minimal buffer stock.

The economic arguments are strong, but so too are the risks.

Stores may work to a one day turnaround (or even less), have to have a fast and dependable supply.

Likewise, the depots have to be geared up for rapid, just-in-time response.
About 70% of Italy's merchandise is moved by road
Truck drivers unions called a 5 day strike as a protest against high fuel prices
Strike called off after 3 days
There were tailbacks on roads into Rome, Milan, Bologna, Naples, Genova. At Ventimiglia, on the Italy-France coastal border, the strikers stopped any trucks from crossing the frontier: 10 km of lorries on the French side. Italian lorry drivers blocked the Frejus tunnel linking France and Italy through the Alps.
Tons of perishable goods left rotting in warehouses
Farmers lost an estimated €50 million per day
Fishermen lost an estimated €40 million per day
General food industry estimated a daily loss of as much as €210 million
Panic buying occurred, and shops and supermarkets began to run out
60% of the petrol stations ran out
In just 3 days!
Medicines kept in central storage and transported to pharmacies once or twice a day as requested

Specialised pharmaceuticals e.g. radio pharmaceuticals for cancer patients or for diagnosis (short half life/shelf life)
Dependent on transport
Many companies outsource software development overseas.

Outsourcing has not been confined to high-tech software development; it extends to application service provisioning.
Outsource computer code

72% of financial services outsource almost half of their development practices

55% of public sector organizations outsource over 40% of code development

Countries known for their ability to develop sophisticated software...India, Pakistan, China, and Russia

Have strong technical capabilities
Large and technically sophisticated labour force and cheaper costs

The chief technology officer of Intel, said the cost of one engineer in the United States would pay for the services of three Indians, four Chinese or five Russians
However, must balance the benefits of outsourcing against the costs,

e especially with regard to security

In a report released by Quocirca, organisations that admitted to being frequently hacked, all outsource at least some of their coding practice

Outsourced software applications can often contain exploitable vulnerabilities
Wargames 1983
Hacking vulnerability trends
The government sector accounted for 25% of all identity-related data breaches
Home users were the most highly targeted sector, accounting for 93% of all attacks
China has 26% of the world's bot-infected computers, more than any other country

Symantec Internet Security Threat Report for July-December 2006
Zombies

bot
(roBOT) Malicious backdoor programs that are specifically designed for use in creating botnets are called bots

botnet
(roBOT NETwork) Also called a "zombie army," a botnet is a large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a DDoS (Distributed Denial of Service) attack
Botnets have vast computing power. They are used as a powerful cyber weapon and are an effective tool for making money illegally. DDoS attacks can also be used as a political tool. In such cases, attacks usually target servers belonging to government organizations. What makes such attacks particularly dangerous is that they can be used as provocation, with a cyber attack on one country being conducted from servers in another country and controlled from a third country.
Estonia:
Capital: Tallinn
Inhabitants: 1.4 mln
EU since 1 May 2004
NATO since 2 April 2004
On 27 April 2007, the Estonian government moved a Soviet-era World War II memorial from the capital city of Tallin to a more secluded location.

Protests erupted in Estonia and Russia.

Weeks of cyber attacks followed, (From 27 April to 19 May 2007) targeting government and private web sites.
The connection has timed out

The server at www.mkm.ee is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again
Targeted Government web sites, mail servers, Internet backbone routers and Banks (over 95% of banking operations are carried out electronically)

Hackers used hundreds or thousands of "zombie" computers and bombarded Estonian Web sites with thousands of requests a second

Sites that typically received 1,000 visits a day had as many as 2,000 a second

Estonia had to cut links to outside world
The government didn't lose any infrastructure

Expensive and time consuming to combat and indicative of weaknesses in Estonia's cyber security

Raised a question in NATO: does mass computer attacks pose a threat to national security?

“We have seen in Estonia that a cyber attack can swiftly become an issue of national security......cyber attacks can cripple societies“

James Appathurai, Nato spokesman
At NATO headquarters in Brussels (14 May)

7 member nations -- Estonia, Germany, Italy, Latvia, Lithuania, Slovakia and Spain -- signed documents formally establishing the Cyber Defence Centre of Excellence in the Estonian capital
The centre will conduct research and training on cyber warfare and include a staff of 30 persons.

“The need for a cyber defence centre to be opened today is compelling, ..... it will help NATO defy and successfully counter the threats in this area”

General James Mattis, NATO’s Supreme Allied Commander
Modern society depends on the operations of civil infrastructure systems, such as transportation, energy and telecommunications.

Infrastructure is becoming more and more interdependent as the economic, technological, and social processes of globalization intensify.

The destruction or disruption of key infrastructures in one EU Member State could cause the loss of lives in another, may have negative effects on the European economy as a whole and might trigger a collapse in public confidence.
The connection has timed out

The server at www.valtsus.ee is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.
This Directive constitutes a first step, in a step-by-step approach to identify and designate ECI and assess the need to improve their protection.

The Directive will initially concentrate on the energy and transport sectors, followed by ICT.

In the years to come the Directive will allow the identification and designation of ECI in all sectors.