Critical Infrastructures

Eng. Luisa Franchina

Lecturers references

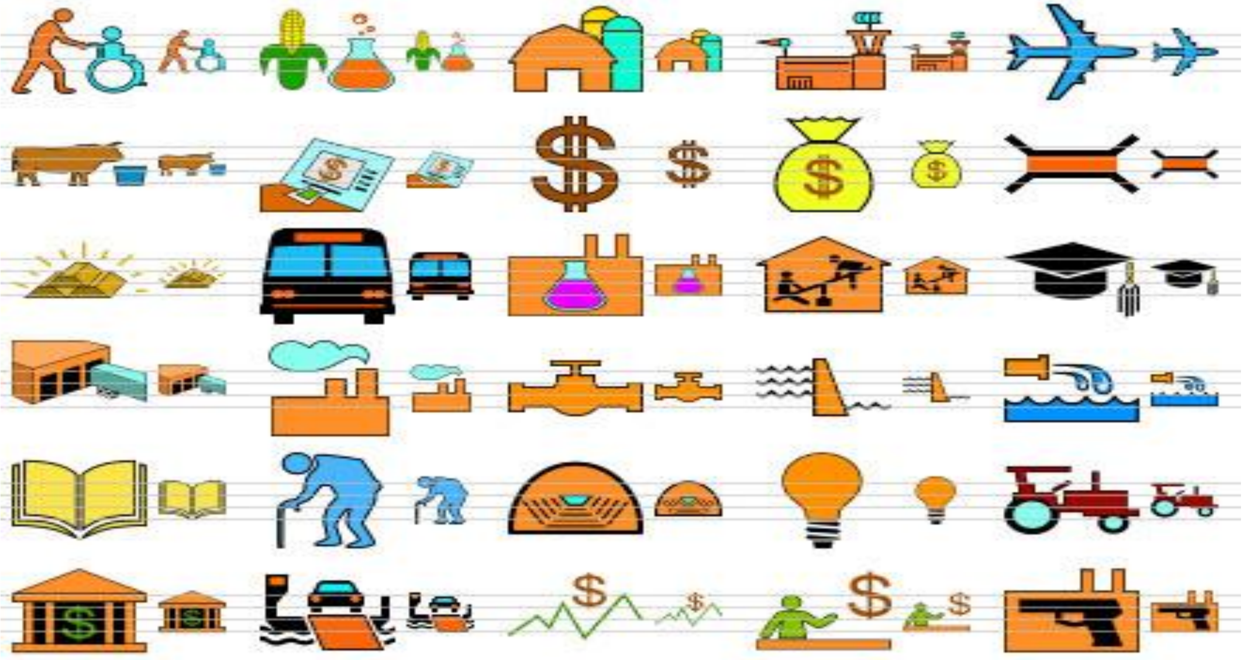
Dr. Angelo Socal (a.socal@hermesbay.com)
Dr. Laura Teodonno (l.teodonno@hermesbay.com)

Hermes Bay SrL

Index

- Definitions
- Metrics: Index Measuring Systems
- Impact evaluation
- Risk assessment and Key Risk Indicators
- Targeting and reverse targeting
- Global risk report

Definitions



EU definitions of Infrastructures and critical infrastructures

The legislative decree 61/2011 related to the identification of the European CI has:

infrastructure: an element, a system or part of it, which supports the maintenance of the functions of society, health, safety and economic well-being;
critical infrastructure (IC): infrastructure, located in a member state of the European Union, which is essential for the maintenance of the vital functions of society, health and health and the population that would have a significant impact in that state, a cause of the impossibility of maintaining these functions

The DPCM 108 2014 related to the golden power (IS) defines:

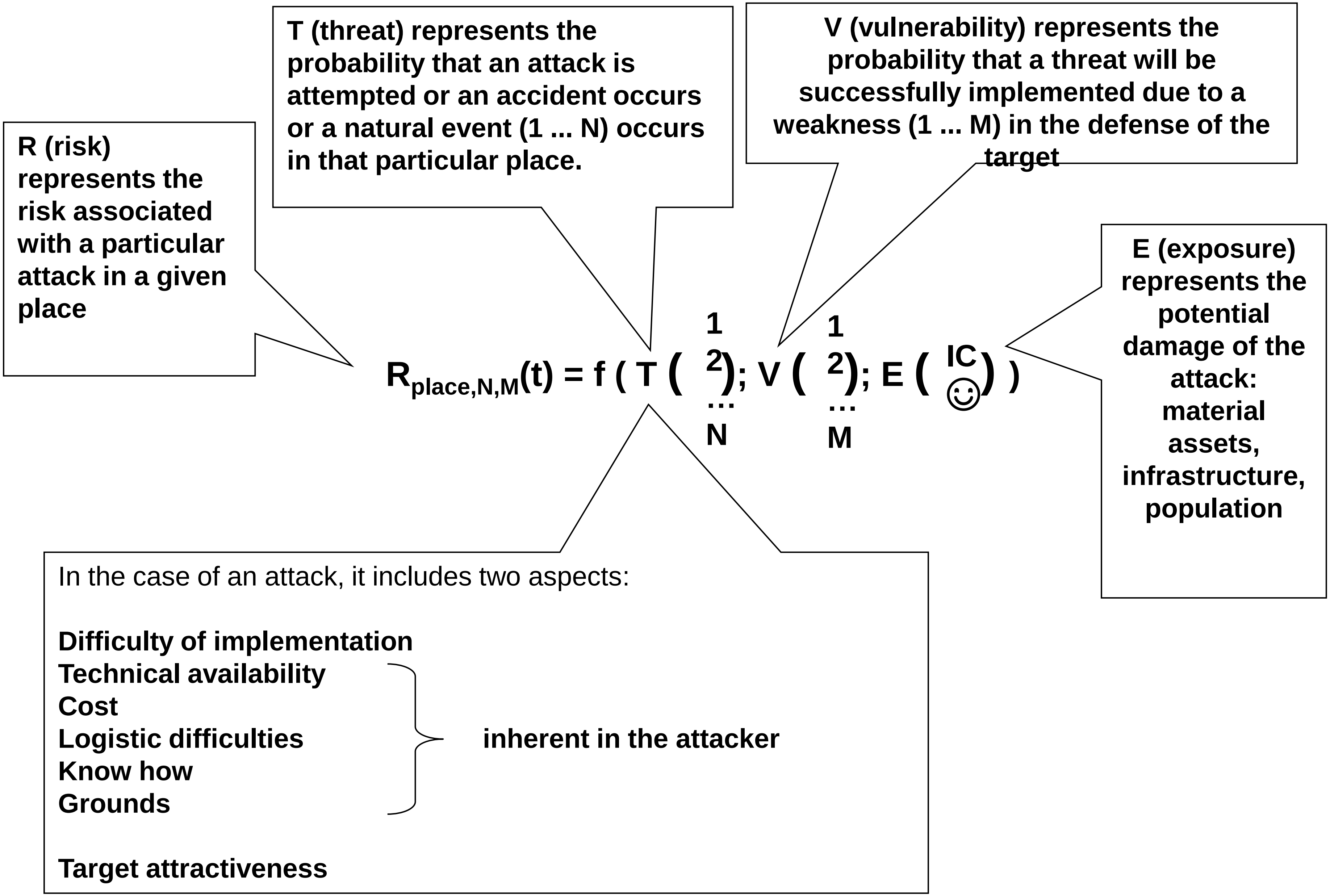
Special powers in the energy, transport and communications sectors
threat of serious injury to public interests related to the security and operation of networks and installations and to the continuity of supply, including the networks and facilities needed to ensure the minimum supply and operation of essential public services
Special powers in the defense and national security sectors
requirement for the exercise of special powers in the security and defense sectors, identified in the existence of a threat of serious injury to the essential interests of defense and national security

Critical Infrsturture Definition & Key Features

- **Each Member State identifies its critical infrastructures on the basis of what they determine essential for the maintenance of vital societal functions, health, safety, security, economic** or **social well-being.**

Examples of critical infrastructures sectors:

- ✓ Water
- ✓ Food
- ✓ Agriculture, forestry and fishing
- ✓ Environment
- ✓ Commerce
- ✓ Culture, icons, aggregation site
- ✓ Energy
- ✓ Finance
- ✓ Industry
- ✓ Information and communication
- ✓ Institution and public administration
- ✓ Health services
- ✓ Services
- ✓ Transport and logistic



R (risk) represents the risk associated with a particular attack in a given place

T (threat) represents the probability that an attack is attempted or an accident occurs or a natural event (1 ... N) occurs in that particular place.

V (vulnerability) represents the probability that a threat will be successfully implemented due to a weakness (1 ... M) in the defense of the target

E (exposure) represents the potential damage of the attack: material assets, infrastructure, population

$$R_{place,N,M}(t) = f\left(T\left(\begin{matrix}1\\2\\\dots\\N\end{matrix}\right); V\left(\begin{matrix}1\\2\\\dots\\M\end{matrix}\right); E\left(\begin{matrix}IC\\\text{☺}\end{matrix}\right)\right)$$

In the case of an attack, it includes two aspects:

Difficulty of implementation
Technical availability
Cost
Logistic difficulties
Know how
Grounds

inherent in the attacker

Target attractiveness

From Risk analysis to Impact analysis

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

$\text{Impact}_{\text{event}}$

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

$\text{Impact}_{\text{domino}}$

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

Hazards

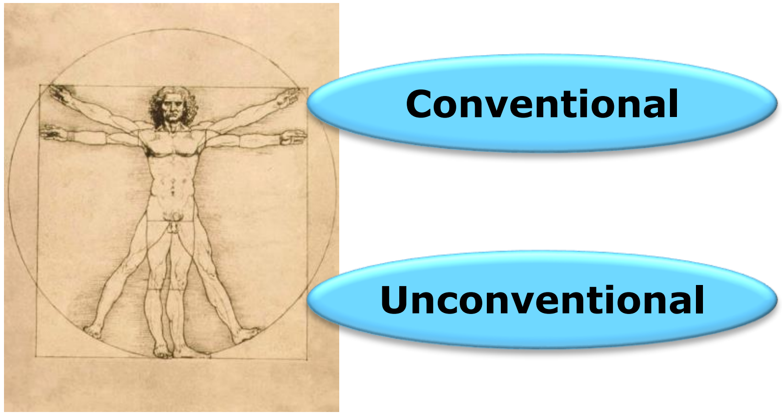
Natural

Predictable and Unpredictable

Dimensions:
Land
Water
Air
Space
Cyber

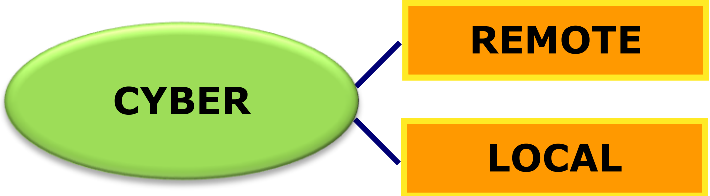
Human

Voluntary and accidental



Conventional

Unconventional



CYBER

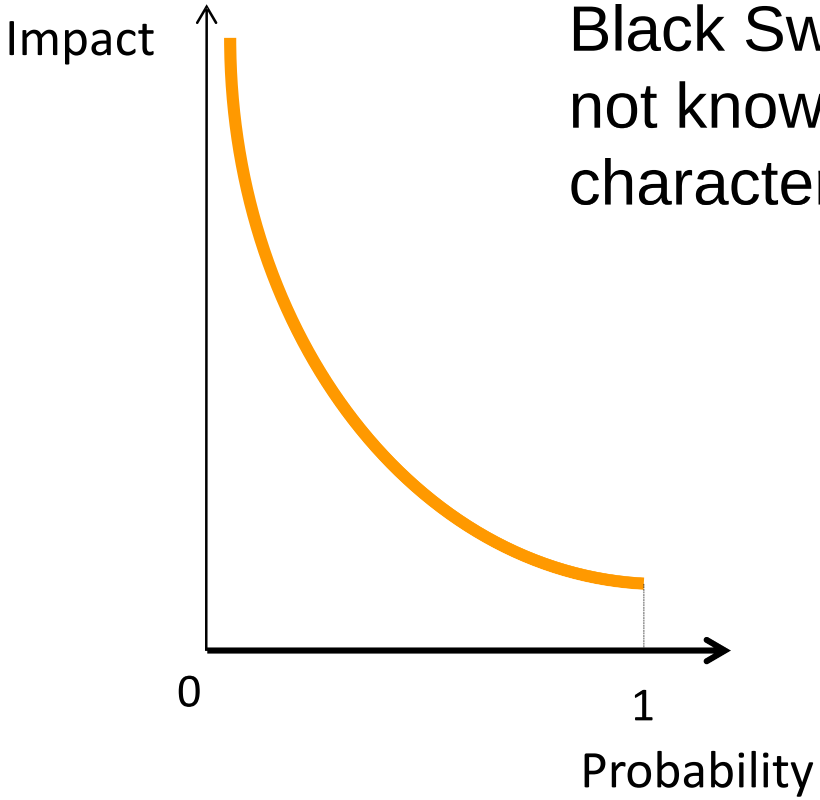
REMOTE

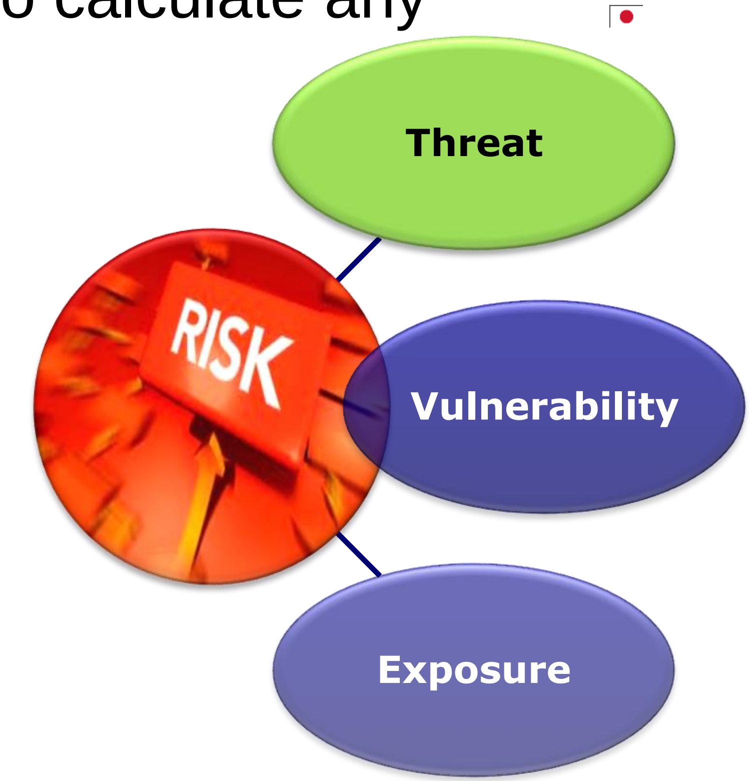
LOCAL

Black swan

Nassim Nicholas Taleb

Black Swan: Event not known, we do not know how to calculate any characteristics



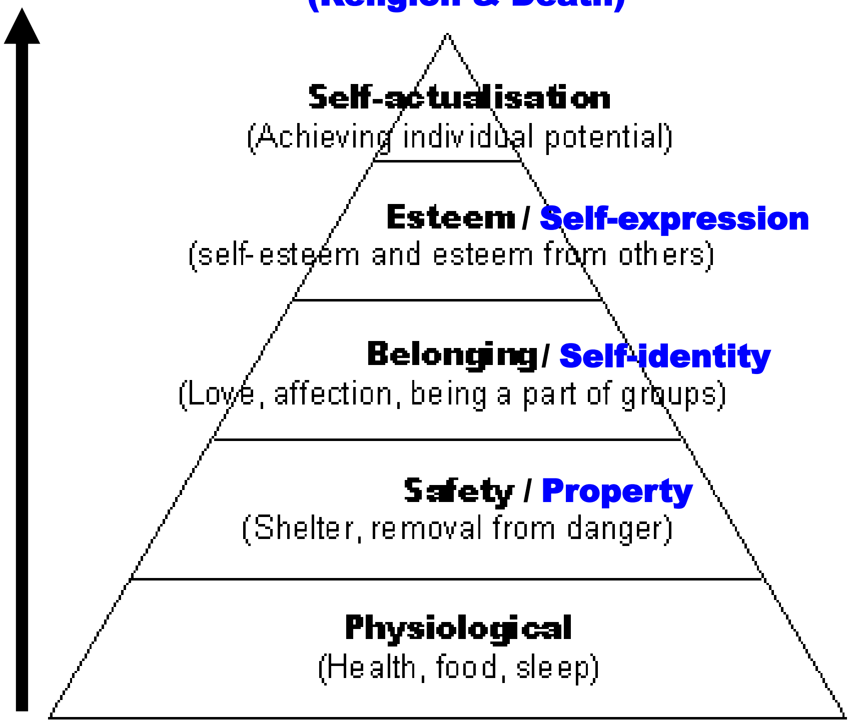


- Anthropic events
- Electromagnetic pulse
- Space climate
- Natural events with a frequency above human memory
- Premonitions and vaunted forecasts
- ...

Maslow’s Hierarchy of Self-Needs
Smart’s Hierarchy of Technoeconomics

Biological Learning Stages

Self-transcendence
(Religion & Death)



Self-actualisation
(Achieving individual potential)

Esteem / **Self-expression**
(self-esteem and esteem from others)

Belonging / **Self-identity**
(Love, affection, being a part of groups)

Safety / **Property**
(Shelter, removal from danger)

Physiological
(Health, food, sleep)

Technological Learning Stages

Biotranscension Society?

Digital Twin IT Society

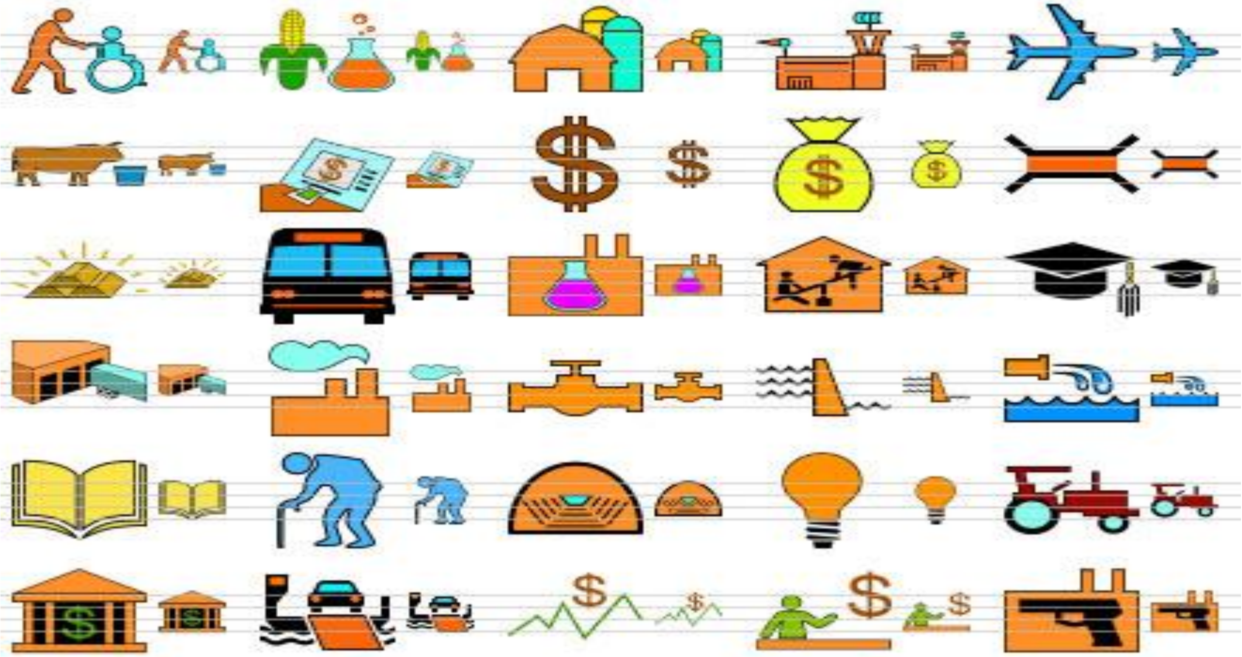
Valuecosm IT Society

Network IT Society

Manufacturing Society

Agricultural Society

Metrics: Index measuring system



Importance of index measuring systems

"When you can measure what you are speaking about…. you know something about it; but when you cannot measure it,… your knowledge of it is of a meager and unsatisfactory kind . . ." --Lord Kelvin (1824-1907)

"If you can't measure it, you can't manage it."

Some questions that decision makers ask themselves:

• Does our approach to security allow the company/critical infrastructure to deal appropriately and appropriately with the risks it runs?

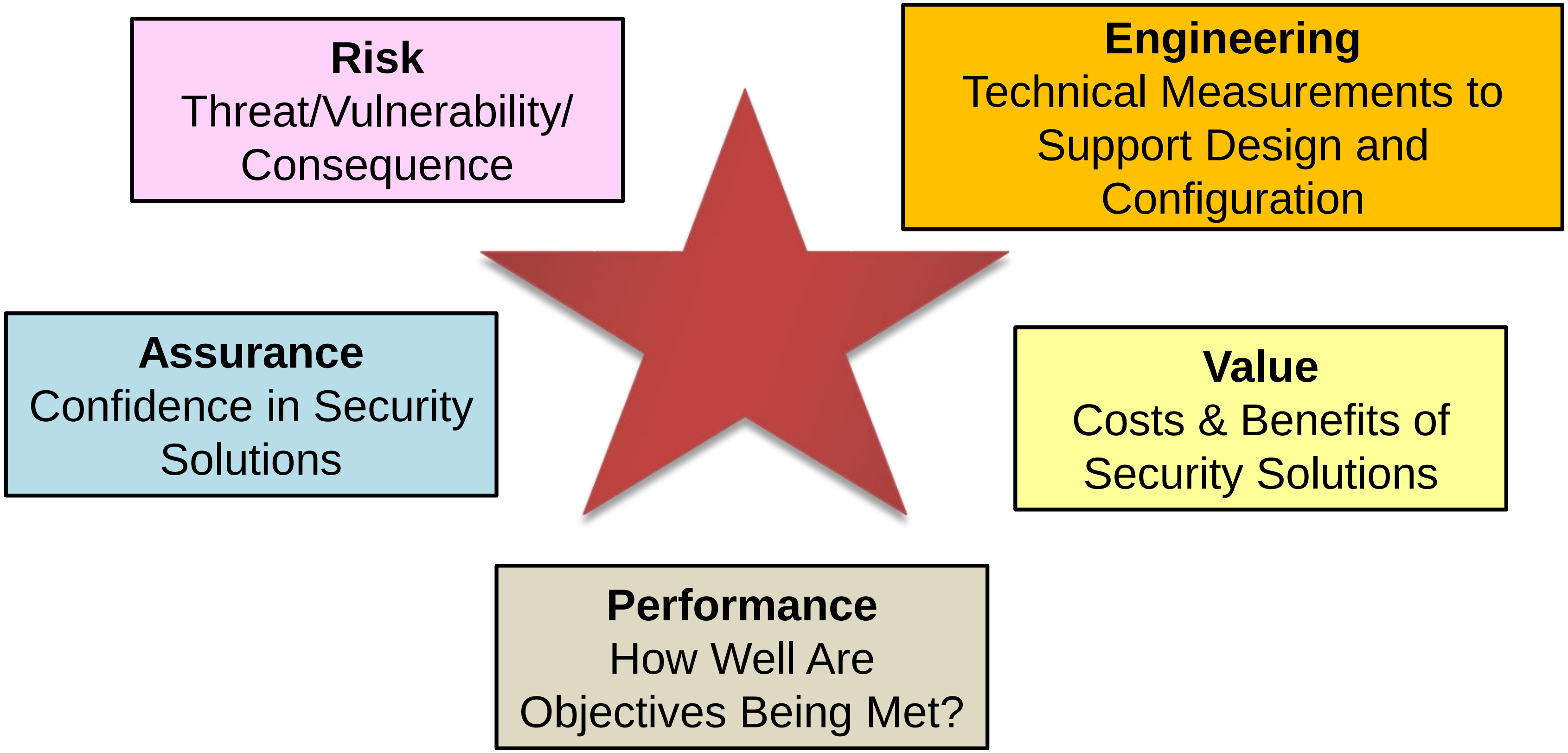
• How is our security approach in line with current standards and how does it compare to industry practices?
• Is our security approach getting better or worse?

• What is our return on investment in security?

Metrics characteristics

- A metric can quickly show hidden and non-obvious aspects of a process or system.
- This metric can take the form of a numerical value, a trend, a position relative to a predefined point, etc. etc.
- However, most often the metrics alone do not have much significance.

Key Security Components



Risk
Threat/Vulnerability/
Consequence

Engineering
Technical Measurements to
Support Design and
Configuration

Assurance
Confidence in Security
Solutions

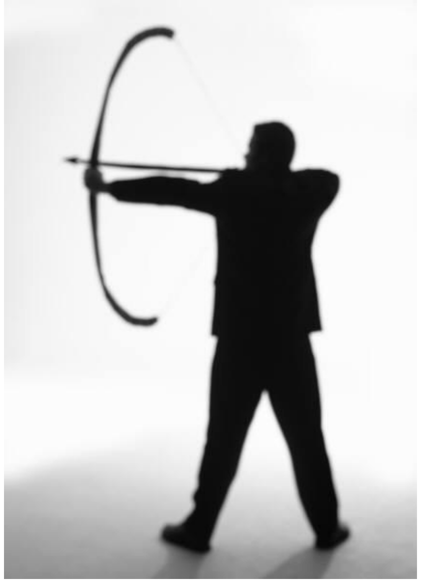
Value
Costs & Benefits of
Security Solutions

Performance
How Well Are
Objectives Being Met?

Security objectives

- The safety objectives are specific to the organization to which they refer and to the control systems.

- In general, security objectives focus on the prevention, detection, mitigation of attacks on their systems and their recovery.



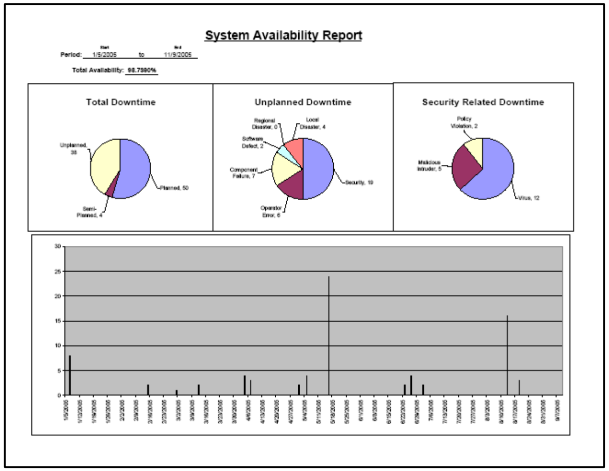
Benchmark

- The benchmarks provide a framework for comparing the measurements or evaluations made.

- They can be taken into consideration as a benchmark:
- Industrial standards;
- Past performance:
- Business objectives;
- Expected performance;
- Statistics on similar products / systems.

Analytics

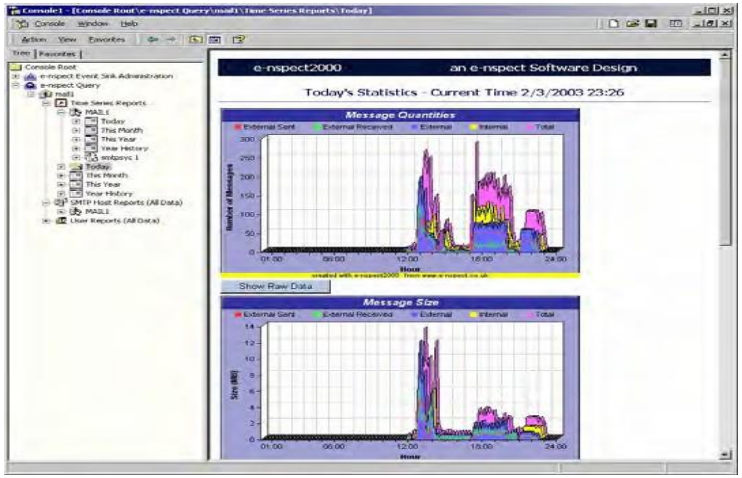
- The metrics can be expressed with a number or with an index for a quicker and simpler analysis (see the dashboards).

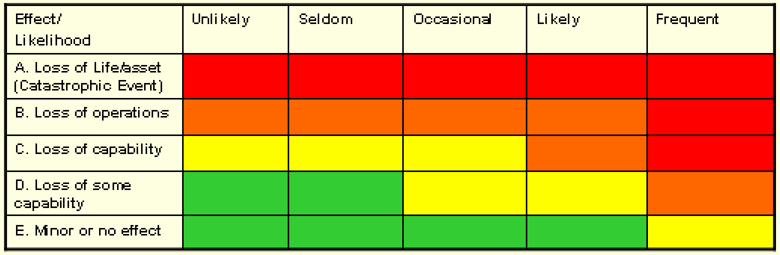


System Availability Report

Period: Start 1/5/2005 to End 11/9/2005

Total Availability: 98.7380%

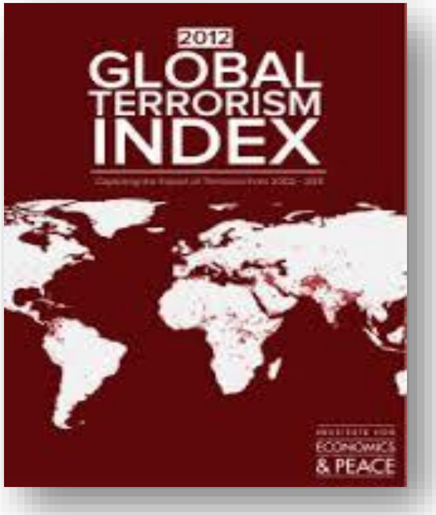




Effect/ Likelihood	Unlikely	Seldom	Occasional	Likely	Frequent
A. Loss of Life/asset (Catastrophic Event)	🟥	🟥	🟥	🟥	🟥
B. Loss of operations	🟧	🟧	🟧	🟧	🟥
C. Loss of capability	🟨	🟨	🟨	🟧	🟥
D. Loss of some capability	🟩	🟩	🟨	🟨	🟧
E. Minor or no effect	🟩	🟩	🟩	🟩	🟨

Impact indicators: an example of measurement for terrorist and security events

The Global Terrorism Index (GTI) aggregates data from the most authoritative sources on terrorism. From its database an integrated scale of results is created that determines the ranking of nations based on the impact of the terrorist acts that occurred.



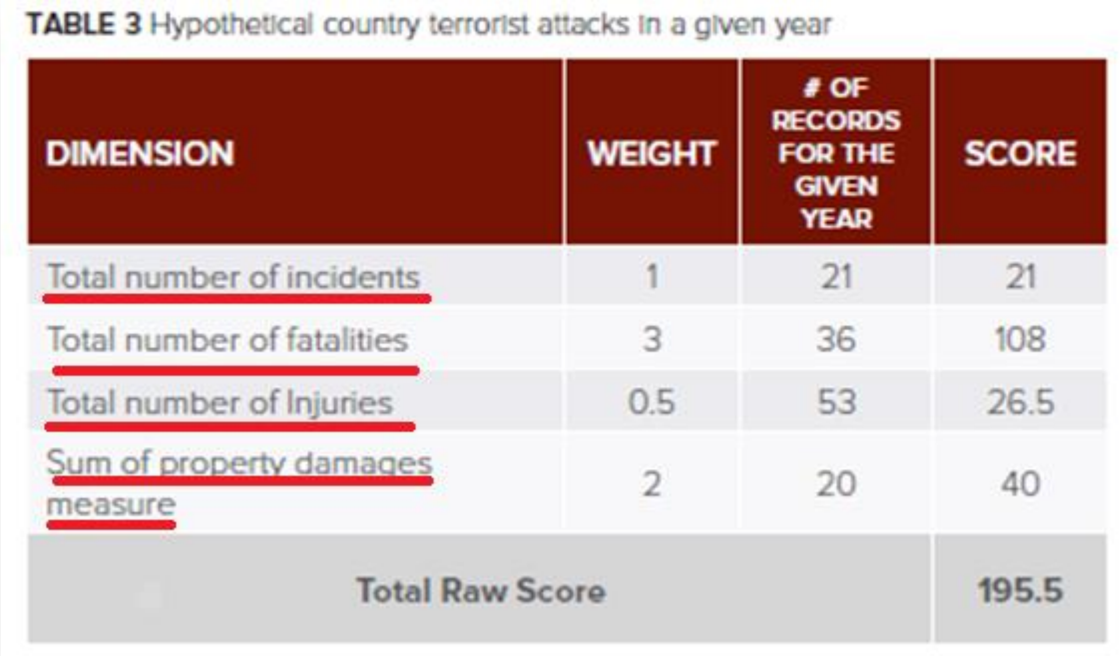
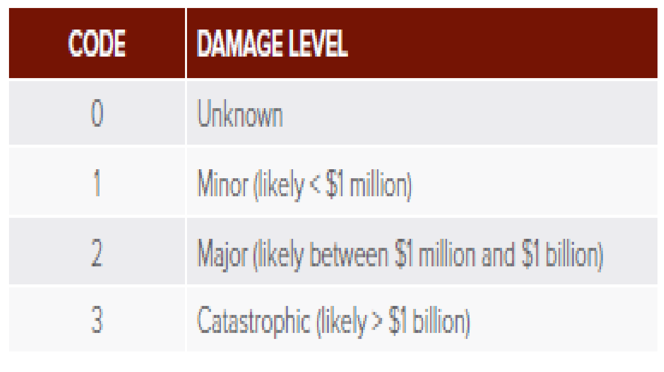


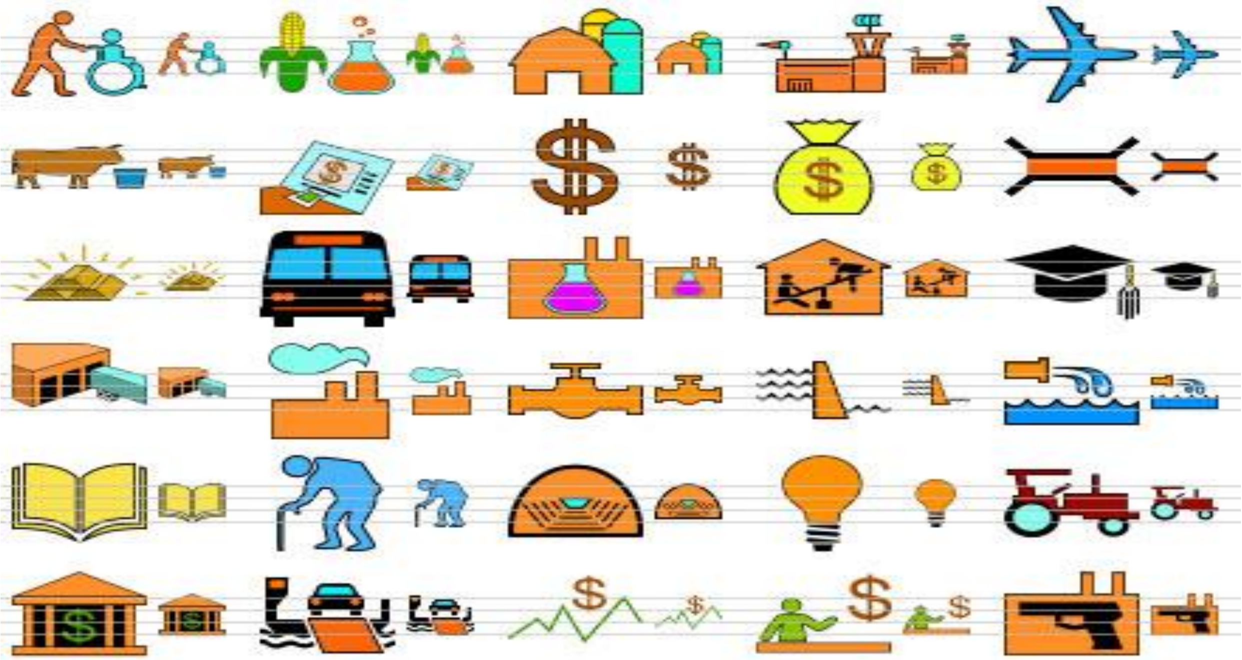
TABLE 3 Hypothetical country terrorist attacks in a given year

DIMENSION	WEIGHT	# OF RECORDS FOR THE GIVEN YEAR	SCORE
Total number of incidents	1	21	21
Total number of fatalities	3	36	108
Total number of Injuries	0.5	53	26.5
Sum of property damages measure	2	20	40
Total Raw Score			195.5



CODE	DAMAGE LEVEL
0	Unknown
1	Minor (likely < $1 million)
2	Major (likely between $1 million and $1 billion)
3	Catastrophic (likely > $1 billion)

Impact evaluation



KPI, KRI, KII, KTI

Key Performance Indicator

- ❑ Metrics relating to the performance and results of the company and its operating units;
- ❑ They represent the performance trend both in real-time and on a daily, weekly, quarterly basis;
- ❑ Show the current position with respect to the achievement of the goal;
- ❑ They can also be used to measure the effectiveness of countermeasures adopted in Risk Management.

Key Risk Indicator

- ❑ Promptly provide information on premonitory or ancillary events of an identified risk;
- ❑ Metrics used to provide timely signals on increasing exposure to a risk;
- ❑ They are built on the basis of eventual identification;
- ❑ In the scorecard, the risk indicators provide a representation of the trend / status of business risks with respect to risk appetite.

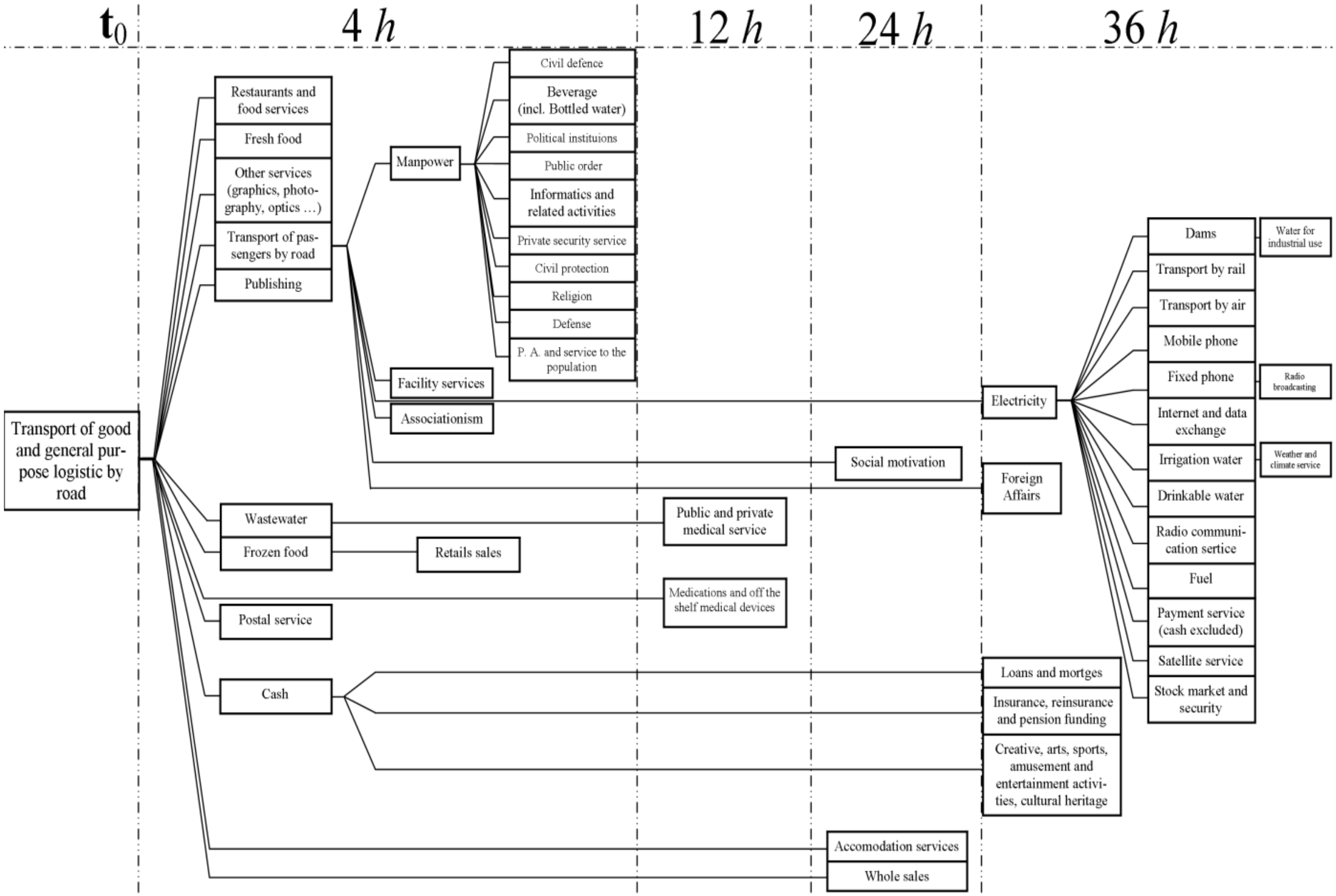
Key Impact Indicator

- ❑ Impact related metrics

Key Threat Indicator

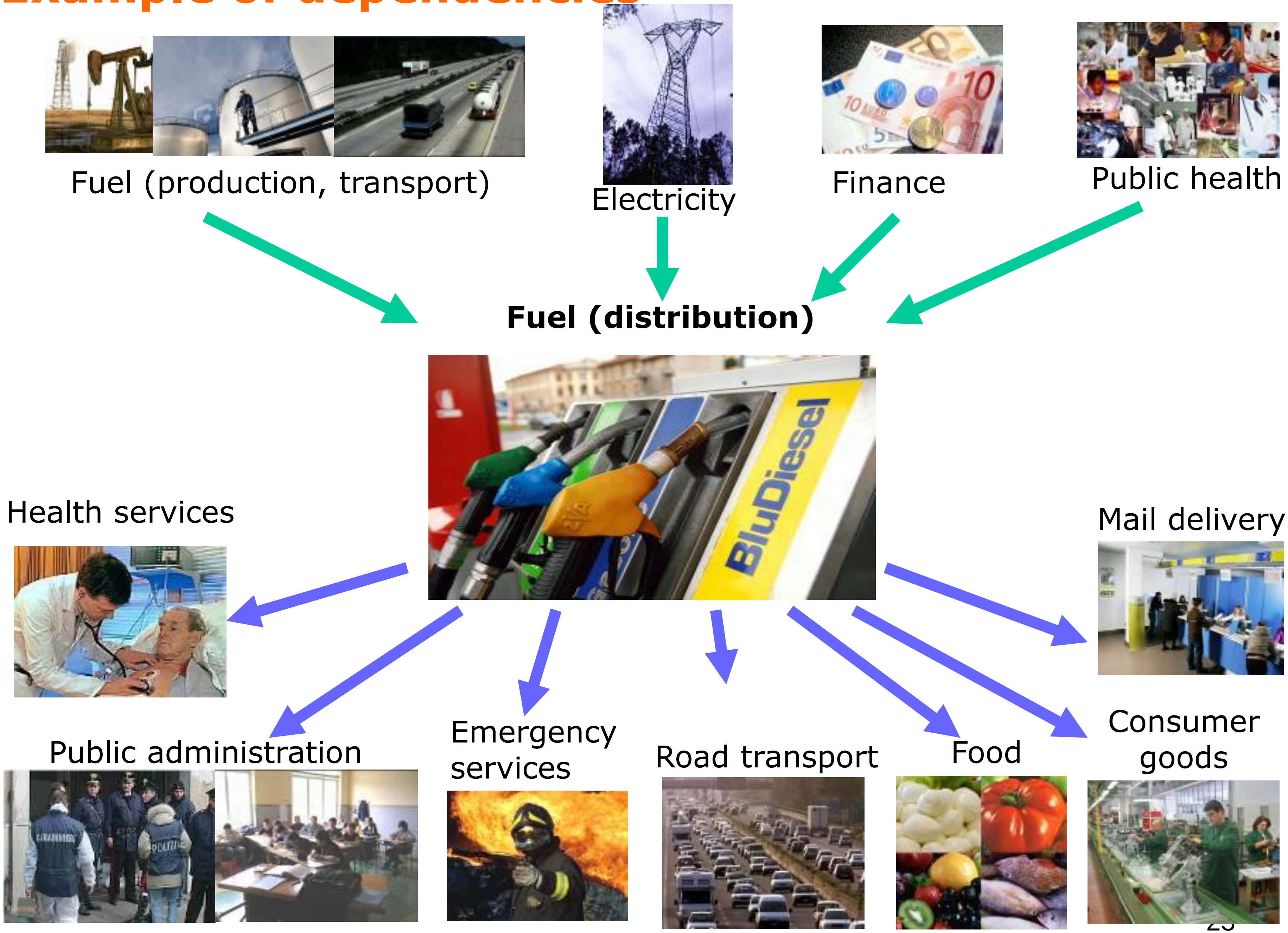
- ❑ Metrics used to provide timely signals on approach / intensification of a threat;

The "external" damage is evaluated on a domino effect basis, adding the damages of each sector involved per unit of time


t_0
4 h
12 h
24 h
36 h
Transport of good and general purpose logistic by road
Restaurants and food services
Fresh food
Other services (graphics, photography, optics …)
Transport of passengers by road
Publishing
Manpower
Civil defence
Beverage (incl. Bottled water)
Political instituions
Public order
Informatics and related activities
Private security service
Civil protection
Religion
Defense
P. A. and service to the population
Facility services
Associationism
Electricity
Social motivation
Foreign Affairs
Dams
Water for industrial use
Transport by rail
Transport by air
Mobile phone
Fixed phone
Radio broadcasting
Internet and data exchange
Irrigation water
Weather and climate service
Drinkable water
Radio communication sertice
Fuel
Payment service (cash excluded)
Satellite service
Stock market and security
Wastewater
Frozen food
Retails sales
Public and private medical service
Medications and off the shelf medical devices
Postal service
Cash
Loans and mortges
Insurance, reinsurance and pension funding
Creative, arts, sports, amusement and entertainment activities, cultural heritage
Accomodation services
Whole sales

Tree of the domino effect generated by "transport of goods by road and logistics"

Example of dependencies



Fuel (production, transport)

Electricity

Finance

Public health

Fuel (distribution)

Health services

Mail delivery

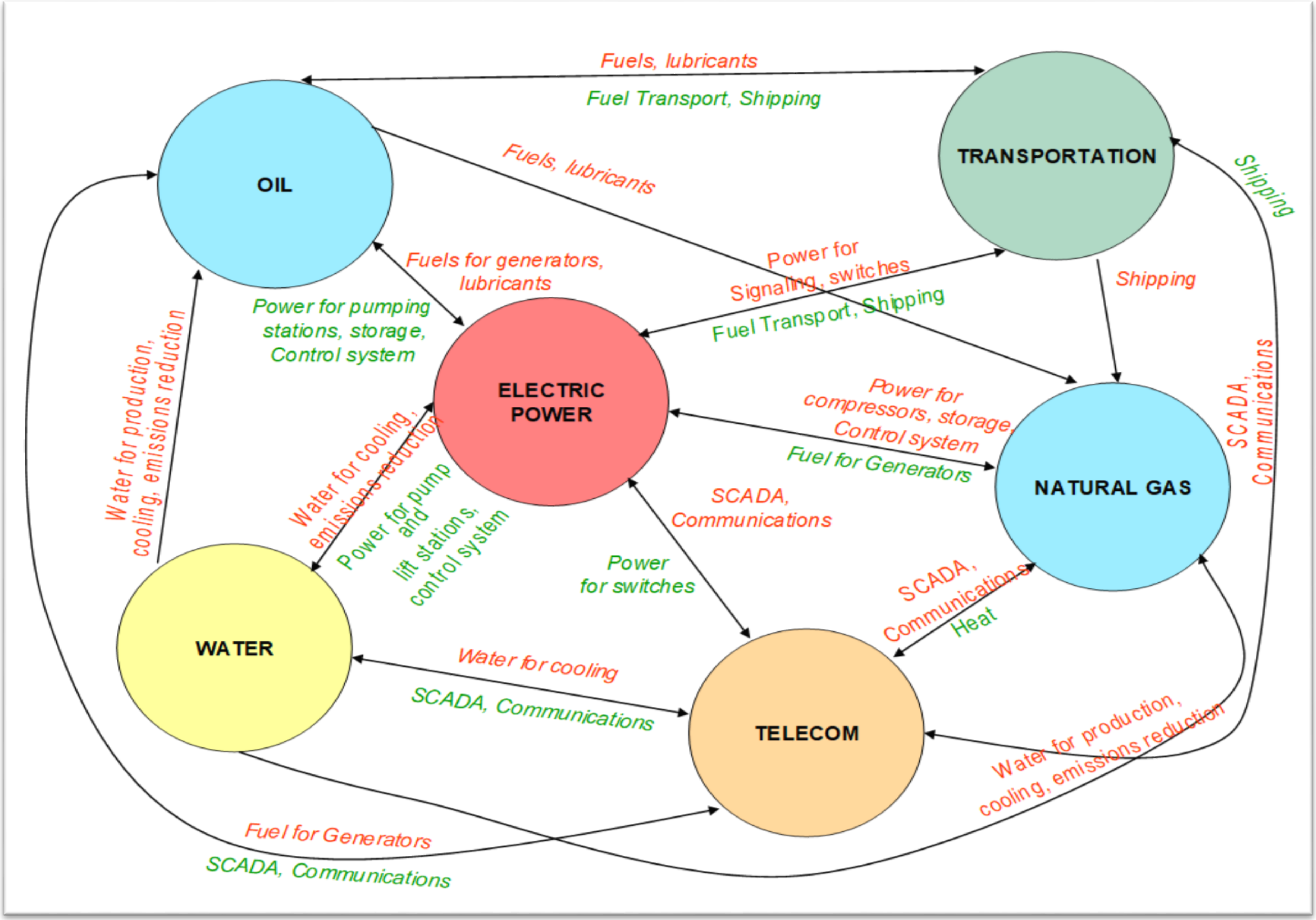
Public administration

Emergency services

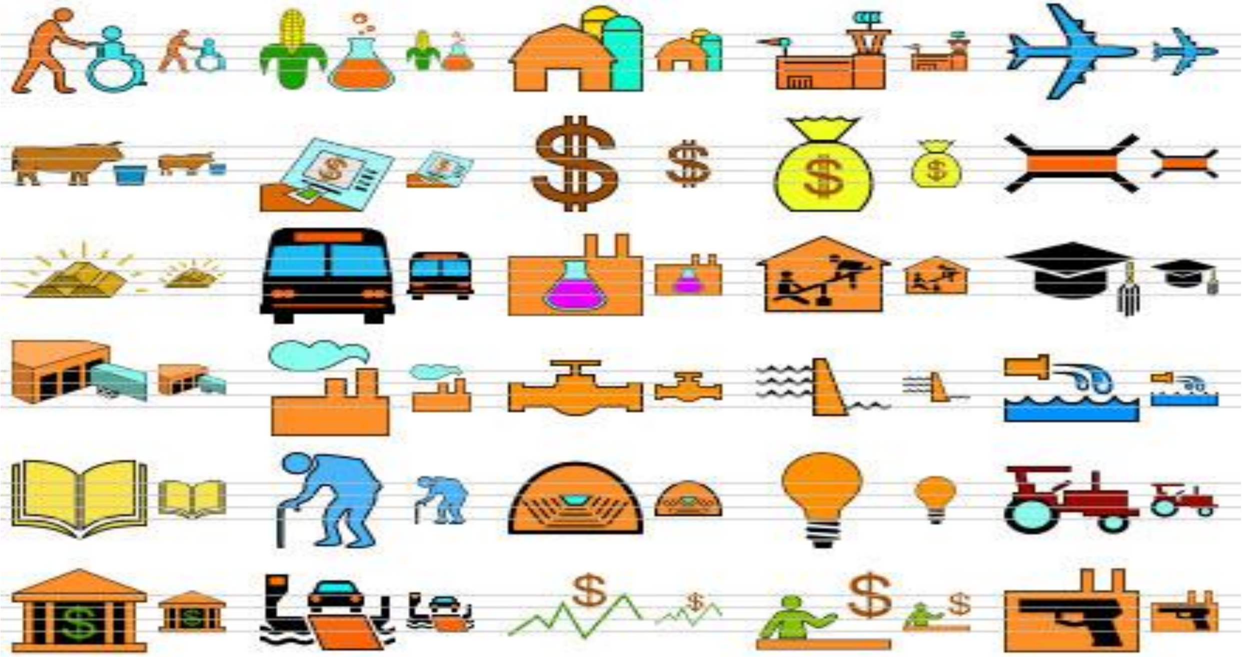
Road transport

Food

Consumer goods

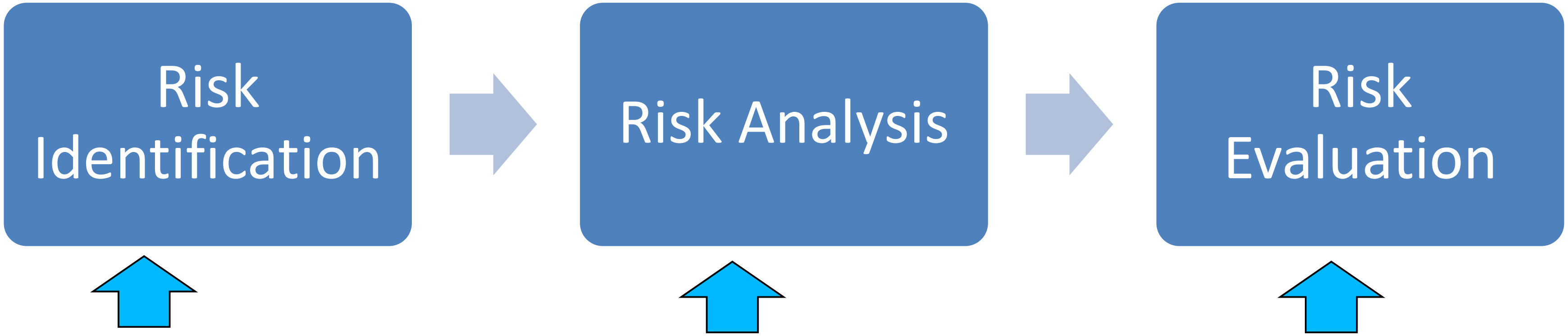

OIL
TRANSPORTATION
ELECTRIC POWER
NATURAL GAS
WATER
TELECOM
Fuels, lubricants
Fuel Transport, Shipping
Fuels, lubricants
Shipping
Fuels for generators, lubricants
Power for pumping stations, storage, Control system
Power for Signaling, switches
Fuel Transport, Shipping
Shipping
Power for compressors, storage, Control system
Fuel for Generators
SCADA, Communications
Water for production, cooling, emissions reduction
Water for cooling, emissions reduction
Power for pump and lift stations, control system
SCADA, Communications
Power for switches
SCADA, Communications
Heat
Water for cooling
SCADA, Communications
Water for production, cooling, emissions reduction
Fuel for Generators
SCADA, Communications

Risk assessment and key risk indicators



Risk Assessment

- ✓ Risk assessment is the overall process of risk identification, risk analysis, and risk evaluation. (ISO 31010)



Risk Identification

Risk Analysis

Risk Evaluation

- ✓ Finding
- ✓ Recognizing
- ✓ Describing risks

- ✓ Comprehend the nature of risk
- ✓ Determine Impact and probability
- ✓ Determine level of risk

- ✓ Prioritizing risk
- ✓ Evaluate whether risk or/and its magnitude is acceptable/tolerable

Risk Assessment – Risk 1/2

- Risks are the combination of the consequences of an event or hazard and the associated likelihood of its occurrence (ISO 31010).

- The consequences are the negative effects of an event expressed in terms of:

  - ✓ **Human impacts**
  - ✓ **Economic and environmental impacts**
  - ✓ **Political/social impacts**

- When the extent of the impacts is independent of the probability of occurrence of the hazard, which is often the case for purely natural hazards, such as earthquakes or storms, risk can be expressed algebraically as:

Risk = hazard impact * probability of occurrence

Risk Assessment – Risk 2/2

- The Impact of an hazard is conditioned by preparedness or preventive behaviors and practices in place, e.g. evacuation plan, contingency plan, security measures etc.
- Impacts are often expressed in terms of **vulnerability** and **exposure**
  - ✓ **Vulnerability V** is defined as the characteristics and circumstances of a community, system or asset that make it susceptible to the damaging effects of a hazard (UNISDR, 2009)
  - ✓ **Exposure E** is the totality of people, property, systems, or other elements present in hazard zones that are thereby subject to potential losses (UNISDR, 2009)
- Therefore Risk can not always be expressed solely as a product between two terms but should be expressed as the following functional relationship:

$$\textbf{Risk} = f(\textbf{ probability of occurrence} * E * V\ )$$

Risk Assessment – Impact Assessment 1/2

In Critical Infrastructure Protection, impact assessment should consider the following type of impacts :

Human impacts

- ✓ the number of affected people
- ✓ the number of deaths,
- ✓ the number of severely injured or ill people,
- ✓ the number of permanently displaced people

Economic and environmental impacts

- ✓ the sum of the costs of cure or healthcare,
- ✓ cost of immediate or longer-term emergency measures,
- ✓ costs of restoration of buildings, public transport systems and infrastructure, property, cultural heritage, etc.,
- ✓ costs of environmental restoration and other environmental costs (or environmental damage),
- ✓ costs of disruption of/to economic activity,
- ✓ value of insurance pay-outs,
- ✓ indirect costs on the economy,
- ✓ indirect social costs, and other direct and indirect costs, as relevant

Risk Assessment – Impact Assessment 2/2

Political/social impacts

- ✓ public outrage and anxiety
- ✓ encroachment of the territory,
- ✓ infringement of the international position,
- ✓ violation of the democratic system,
- ✓ social psychological impact,
- ✓ impact on public order and safety,
- ✓ political implications, psychological implications,
- ✓ damage to cultural assets,
- ✓ other factors considered important which cannot be measured in single units

Political/social impacts will generally refer to a semi-quantitative scale comprising a number of classes

🟩 limited/ insignificant

🟩🟨 minor/ substantial

🟨🟨🟨 moderate/ serious

🟨🟨🟥🟥 significant/ very serious

🟥🟥🟥🟥🟥 catastrophic/ disastrous.

Risk Assessment – Empirical Evidence

- Impact analysis should rely as much as possible on **empirical evidence and experience from past event data or established quantitative models of impact**. It is clear that for quantification purposes, a number of assumptions and estimates will have to be used, some of which may be rather uncertain. These **assumptions and estimates should always be clearly identified and substantiated.**

- The assessment of the probability of an event or hazard should be based, where possible, on the historical frequency of events of similar scale and available statistical data relevant for an analysis of the main drivers.

- However, when considering Cyber-Threat, reliance on historical data may not be enough, especially when considering the most innovative and advance threats (APT, Zero day, etc.). For this reason in this domain the focus of risk assessment has shifted toward continuous monitoring and real-time data gathering/analysis

Risk Assessment – Single & Multiple

- ✓ **Single-risk assessment**: determine the singular risk (i.e. likelihood and consequences) of one particular hazard (e.g. flood) or one particular type of hazard (e.g. flooding) occurring in a particular geographic area during a given period of time.

- ✓ **Multi-risk all-hazard assessment:** determine the total risk from several hazards either occurring at the same time or shortly following each other, because they are dependent from one another or because they are caused by the same triggering event or hazard; or merely threatening the same elements at risk (vulnerable/ exposed elements) without chronological coincidence.

Single-Risk Assessment

- **Single-risk assessments**:

  - ✓ Single-risk analysis estimates the risk of a singular hazard in isolation from other hazards or risk scenarios. Different natural hazards require very different analyses of their risk, i.e. in establishing the probability of their occurrence and the level of possible impacts.

  - ✓ EU legislation has introduced a number of "single-hazard" risk assessment requirements, such as in the area of flood risks, droughts, risks of accidents with dangerous substances, and risks to European Critical Infrastructures.

- However, for **Critical Infrastructure Protection** a **multi-risk all-hazard** approach is required in order to gain a multi-hazard and a multi-vulnerability perspective.
- Each risk assessment must incorporate **possible amplifications due to the interaction with other hazards**;
- Many single-risk analyses consider to varying degrees the complexity of different origins of a particular hazard. But they often **stop short of bringing together dissimilar hazards and considering adequately infrastructures interdependencies**.

Multi-risk all-hazard risk assessments

Multi-risk assessments determine the total risk from several hazards, taking into account possible hazards and vulnerability interactions:

A. occurring at the same time or shortly following each other,

- ✓ because they are dependent of one another
- ✓ because they are caused by the same triggering event or hazard;

Also referred to as follow-on events, knock-on effects, domino effects or cascading events

The likelihood of each of the events occurring is of course correlated to the likelihood of occurrence of the other event or the prior triggering event.

B. threatening the same elements at risk (vulnerable/ exposed elements) without chronological coincidence

In both cases the assessment of consequences then needs to consider the cumulative impacts of all of the various impacts occurring at the same time or shortly following each other.

Multi-Risk Assessment Challenges

- ➢ Current Challenges:
  - ✓ Adequately taking into account all possible follow-on effects (also: knock-on effects, domino effects or cascading effects) amongst hazards and infrastructure (Interdependencies)
  - ✓ Co-ordination and interfacing between different specialized authorities and agencies, which each deals with specific hazards or risks without developing a complete overview of the knock-on, domino and cascading effects
  - ✓ Most multi-risk assessment methodology are just an adaptation of single risk-assessment methodology
    - ✓ There are a number of difficulties combining single-risk analyses into more integrated multi-risk analysis:
    - ✓ Available data for different single risks may refer to different time windows, different typologies of impacts are used, etc.,
    - ✓ makes comparisons and rankings difficult if not impossible.

Risk Assessment & Critical Infrastructure Protection

- Risk assessment is the key element in Critical Infrastructure Protection

- Risk assessment is indispensable in order to:
  - ✓ Identify **threats/hazard,**
  - ✓ **Assess vulnerabilities**
  - ✓ **Evaluate the impact on assets, infrastructures or systems** taking into account the **probability of the occurrence** of these threats/hazards

- There is a significant number of risk assessment methodologies for critical infrastructures protection.

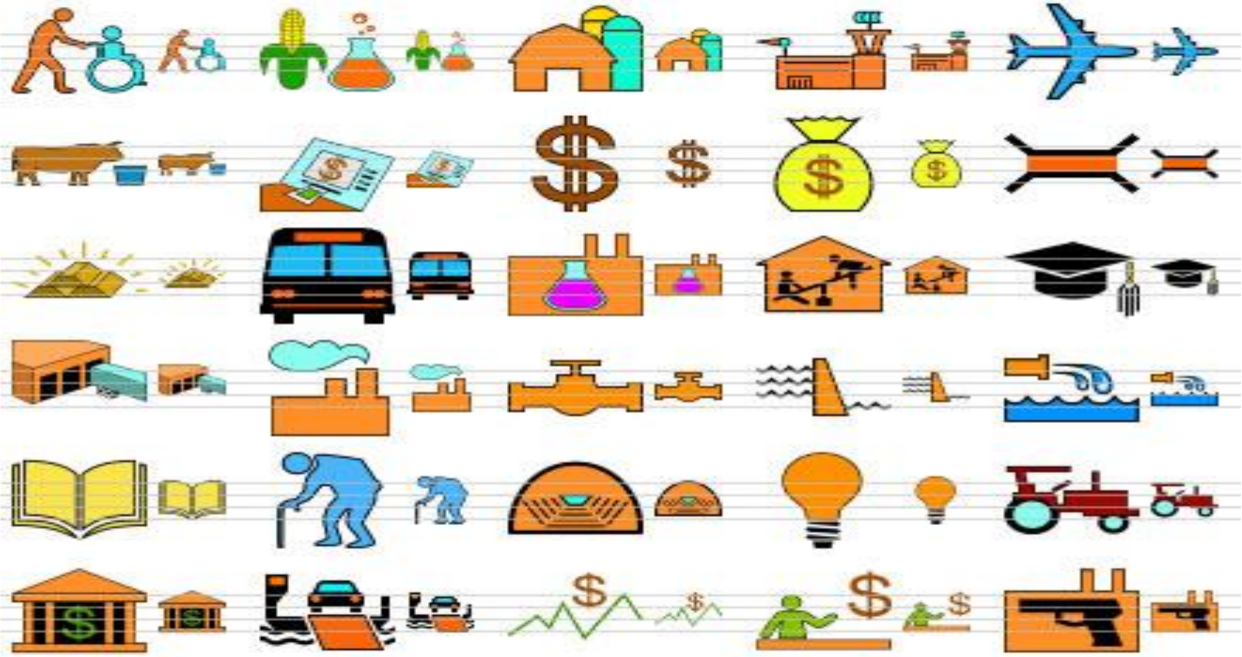
- Critical Infrastructure risk assessment methodologies differ in scope, audience to which they are addressed and their domain of applicability.

Risk Assessment Metodologies for Critical Infrastructure Protection

The following are the Methodologies that will be presented:

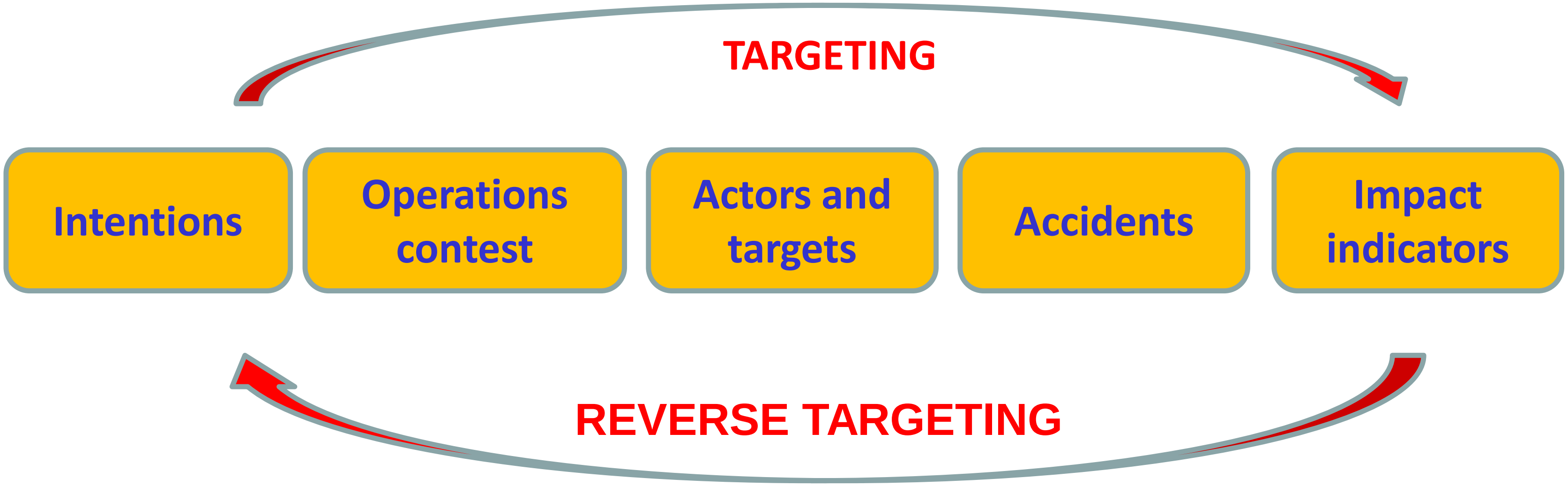
- **CARVER(S)**
- **MSHARPP**

Targeting and reverse targeting



Targeting and reverse targeting

- ❑ Conducting a targeting activity means making a clear choice on the objectives to be attacked for reasons of efficiency (cost-benefit)
- ❑ Both are united by the elements they intend to study: actors, objectives, impact indicators
- ❑ Targeting identifies indicators to attack a certain goal, reverse targeting tries to identify «post mortem» what happened, how and why



CARVER(S) E MSHARPP

- Military derivation tools
- They express a judgment about the attractiveness and vulnerability of targets in order to allocate resources efficiently relative to the target to be attacked
- Impact assessment
- Targeting and decision support tools
- Attackers vs defenders? Goals and weaknesses / attack zones
- Target vs asset

CARVER(S) 1/2

The CARVER (S) matrix was developed by the US Special Forces during the Vietnam War.

In the Risk / Vulnerability assessment area it is used to define the level of vulnerability of the target and to efficiently orient its resources in relation to the type of target.

CARVER (S) can be applied both in attack and defense perspective.

C	CRITICALITY
A	ACCESSIBILITY
R	RECUPERABILITY
V	VULNERABILITY
E	EFFECT
R	RECOGNIZABILITY
S	SHOCK

CARVER(S) 2/2

CRITICALITY ⇨ Depending on the context of reference, it indicates the estimate of the impact (human or economic) deriving from a potential attack.

ACCESSIBILITY ⇨ Possibility, by the attacker, to physically access the lens.

RECUPERABILITY ⇨ Possibility, by the attacked system, to recover the initial functions**.**

VULNERABILITY ⇨ Indicates the degree of vulnerability of the target.

EFFECT ⇨ It is the quantifiable impact (economic, reputational, etc.) of an attack.

RECOGNIZABILITY ⇨ It is the degree of ease with which the attacker can identify his target.

SHOCK ⇨ Originally related to environmental impacts or agriculture, it can indicate the symbolic and psychological aspects of an attack.

CRITICALITY

- Identify critical assets and single points of failure
- It represents the value of the target or the relevance of a system, or the degree of "damage" on the target
- Some variables:
- impact time
- amount of damage
- backup of services
- target number
- the positions of the targets

Criteri della criticità	Scala
Loss of over 10 thousand lives; immediate arrest of activities; the target no longer works	9-10
Loss between 1000 and 10 thousand lives; stoppage of activities within one day; 66% reduction in activities	7-8
Loss between 100 and 1000 lives; arrest within 1 week; 33% reduction in activities	5-6
Loss of lives less than 100; arrest within 10 days; 10% reduction in activities	3-4
No loss of life; there are no significant effects on the activities	1-2

ACCESSIBILITY

- Degree of ease of access to assets or achievement of objectives
- Both physically and with remote weapons;
- It depends:
- from the possibility of access / exit and survival / escape of the attacker
- from the security frame around the target

Criteri dell’accessibilità	Scala
Accesso facile (limitate barriere umane, accesso illimitato, fonti di informazioni disponibili)	9-10
Accessibile (limitate barriere umane, accesso per un’ora, fonti di informazioni limitate)	7-8
Parzialmente accessibile (sotto costante osservazione umana, presenti barriere fisiche, fonti di informazioni non specifiche)	5-6
Difficilmente accessibile (osservazione umana stabile, accesso controllato, limitate fonti di informazioni	3-4
Non accessibile (barriere fisiche e umane efficienti, accesso ben controllato non ci sono informazioni sul target)	1-2

RECUPERABILITY

- Indicates the time needed to repair or restore the asset from damage
- In assessing resilience, each target also provides an estimate of the attacker's motivations (who can attack him?)
- The concept refers to material damage and not to people

Resilience criteria	scale
More than one year	9-10
6-12 months	7-8
3-6 months	5-6
1-3 months	3-4
Less than one month	1-2

VULNERABILITY

- Who attacks: ability, resources and intentions of the opponent
- Who defends himself: countermeasures
- It depends:
- from the nature and from the establishment of the target;
- from the amount of damage;
- from the available resources;
- from the personality, experience and mental attitude of the adversary

Criteri della vulnerabilità	Scala
Facile introduzione di sufficienti agenti di minaccia	9-10
Introduzione di sufficienti agenti di minaccia	7-8
Introduzione di agenti probabile per il 30-60%	5-6
Introduzione di agenti probabile per il 10-30%	3-4
Introduzione di agenti probabile per meno del 10%	1-2

EFFECT

- It is defined as "the purpose and magnitude of the adverse consequences following an attack"
- Represents the quantifiable impact of an attack
- It is inversely proportional to the number of structures producing the same result
- Among the variables:
- the real activation of countermeasures
- unemployment
- collateral damage

Criteri dell’effetto	Scala
Più del 50% del sistema è stato colpito	9-10
Il sistema è stato colpito per un 25-50%	7-8
Il sistema è stato colpito per un 10-25%	5-6
Il sistema è stato colpito per un 1-10%	3-4
Il sistema è stato colpito per meno dell’1%	1-2

RECOGNIZABILITY

- Represents the degree to which a target can be recognized unequivocally
- A retrospective assessment is performed in the adversary's shoes
- factors:
- size and complexity of the target
- presence of distinctive elements (symbols, emblems, trademarks)
- degree of technical sophistication
- the attacker's experience

Criteri del riconoscimento	Scala
Il target è chiaramente riconoscibile	9-10
Il target è facilmente riconoscibile	7-8
Il target è difficile da riconoscere e può essere confuso	5-6
Il target è difficile da riconoscere ed è facilmente confuso con altri target	3-4
Il target non può essere riconosciuto se non da esperti	1-2

SHOCK

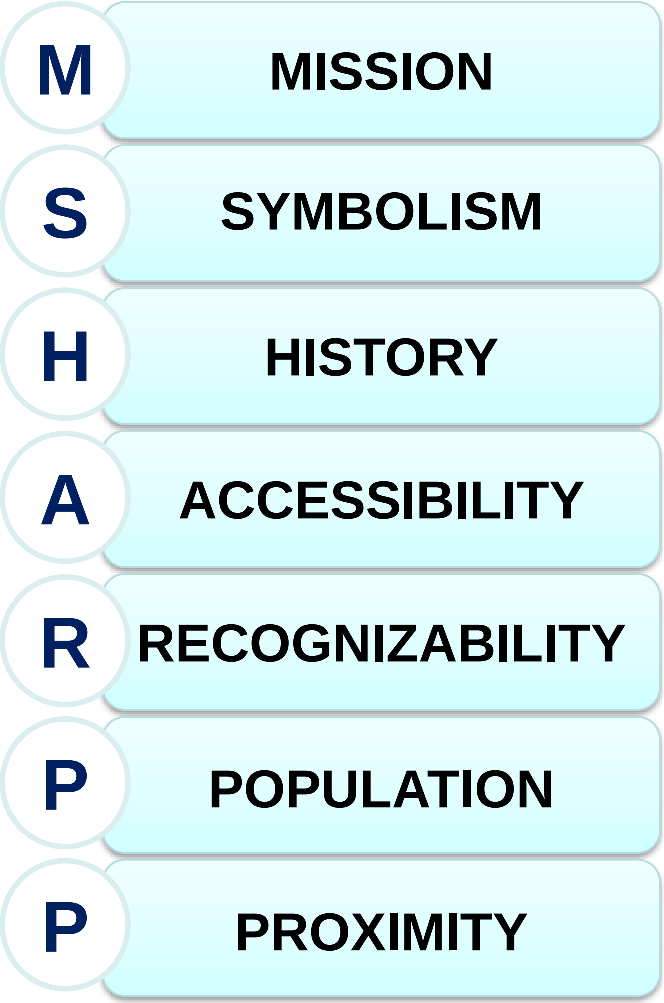
- It is important to evaluate all the consequences of an attack
- Combines health, psychological aspects and collateral national economic impacts (structural downgrade): it must be considered at national / systemic level
- Not only the number of victims but also if the target has a historical, cultural, religious or symbolic meaning or if the victims belong to some categories of subjects (children, the elderly)
- Four variables:
- destruction of symbolic targets
- large number of victims
- a sensitive nature of the targets
- ability to hit values and emotions at heart

Criteri dello shock	Scala
Estrema rilevanza simbolica e impatto economico	9-10
Grande rilevanza simbolica e impatto economico	7-8
Moderata rilevanza simbolica e impatto economico	5-6
Limitata rilevanza simbolica e impatto economico	3-4
Non ha una rilevanza storica né un impatto economico	1-2

MSHARPP 1/2

The MSHARPP scheme is another matrix that can be used to evaluate the intrinsic vulnerabilities and the exposure level of an asset (material, immaterial, human); both in an attack and a defense perspective.

When using the MASHARPP scheme, an assessment is made of elements such as the degree of "attractiveness" of a potential target, the means available to access it, the nature of the impact, the possible involvement of other assets, etc.



M MISSION

S SYMBOLISM

H HISTORY

A ACCESSIBILITY

R RECOGNIZABILITY

P POPULATION

P PROXIMITY

MSHARPP 2/2

MISSION ⇨ It indicates the ability (eg by a company) to continue to provide services in an optimal manner towards the population, public institutions, etc.

SYMBOLISM ⇨ It pertains to the symbolic / iconic aspects of the target of a potential attack.

HISTORY ⇨ It is possible to estimate the degree of sensitivity of the objective from the evaluation of the "historical" of the attacks that took place previously.

ACCESSIBILITY ⇨ Possibility, by the attacker, to physically access the lens.

RECOGNIZABILITY ⇨ Degree of ease with which the attacker can identify his target.

POPULATION ⇨ Amount of population affected through the attack on the target.

PROXIMITY ⇨ The geographical proximity of the potential target to other buildings of strategic importance or densely populated areas.

MISSION

- It takes into consideration the location, activities, capabilities and resources of the target
- Three elements:
- relevance (area and asset value)
- the effect (psychological, economic, sociological aspects and military impacts)
- the resilience (time required to recover the functions of the target)

Criteri della missione	Scala
Il target non può continuare a svolgere la sua missione	5
La missione del target è compromessa dall'attacco	4
Metà della missione del target rimane attiva	3
Il target potrebbe continuare a svolgere la sua missione anche se con un certo grado di inefficacia	2
La distruzione della missione dell'asset non ha effetti sul compimento della missione	1

SYMBOLISM

- Consider if the target represents (or is perceived as) a symbol of a certain reality (State, military apparatus, private companies)
- It can acquire symbolic value for both the adversary and the local community
- The place / area is a key factor

Criteri del simbolismo	Scala
La posizione del target è un simbolo ben preciso delle intenzioni dell'avversario	5
Il target ha un significato storico, religioso o simbolico da difendere	4
Il target è considerato dal difensore come un punto forte invulnerabile	3
Il target è associato alla capacità produttiva o economica del difensore	2
Il target è considerato dal difensore come una popolare area di raccolta	1

HISTORICAL

- Previous experiences, similar attacks in history
- Focus attention not only on the history of similar attacks but also on local criminal reports
- Role of Lessons learned

Criteri della storicità	Scala
Attacchi contro questi target sono condotti in maniera routinaria e con minacce note	5
Attacchi contro questi target in maniera routinaria e con minacce per lo più dirette	4
Attacchi contro questi target sono capitati	3
Questi target sono stati minacciati da tali attacchi	2
Attacchi contro questi target corrispondono a come noi ci immaginiamo il potenziale funzionamento delle minacce	1

ACCESSIBILITY

- Degree of ease of access to assets / achievement of objectives
- Critical paths to reach the target are identified and studied
- The attacker must not only reach the target but also be able to stay there for a period of time

Criteri dell’accessibilità	Scala
Facilmente accessibile, le difese possono essere sviluppate	5
Il target è dentro un perimetro ma all’aperto	4
Il target è dentro una costruzione ma al piano terra	3
Il target è dentro una costruzione ma al secondo piano	2
Il target non è accessibile o è accessibile solo con estrema difficoltà	1

RECOGNIZABILITY

- Degree with which the target can be visually recognized or if information on the target is available
- Weather conditions (snow, fog, rain) play an important role as well as the road to reach the target (forest, vegetation)
- Some variables:
- the distance
- the light
- season
- the existence of distinctive elements

Criteri del riconoscimento	Scala
Il target è chiaramente riconoscibile	5
Il target è facilmente riconoscibile	4
Il target è difficile da riconoscere di notte o col cattivo tempo o può essere confuso con altri target	3
Il target è difficile da riconoscere di notte o col cattivo tempo e può essere facilmente confuso con altri target	2
Il target non può essere riconosciuto sotto nessuna condizione	1

PROXIMITY

- Frames the location of the target. Is the target close to other personal / citizenship, structures, resources? Is there a risk of collateral damage to other nearby targets?
- Nearby are there national monuments and / or religious symbols that the enemy takes into consideration?
- A target-rich environment can increase the likelihood of an attack

Criteri della prossimità	Scala
Il target è in prossimità di altri target; ingenti rischi, vittime, distruzione totale di strutture e personale	5
Il target è in prossimità di altri target; ingenti rischi, vittime, distruzione parziale di strutture e personale	4
Il target è appena in prossimità	3
Il target è parzialmente isolato	2
Il target è isolato; non ci sono rischi per altro personale, strutture o eventuali riferimenti simbolici	1

POPULATION

- Quantity of population
- The "demography" of the population: who can be the targets? Are they part of a particular social group? Are they civil / military? Are they part o a religious movement? What nationalities are they?

Criteri del riconoscimento	Scala
L’attacco causa più di 1000 vittime, un impatto significativo a livello internazionale e per le infrastrutture	5
L’attacco causa più di 500 vittime, un impatto significativo a livello internazionale e per le infrastrutture	4
L’attacco causa più di 100 vittime, un impatto apprezzabile a livello internazionale e per le infrastrutture	3
L’attacco causa più di 10 vittime e un basso impatto a livello internazionale e per le infrastrutture	2
Non ci sono persone presenti e non sono registrati danni per le infrastrutture critiche	1

Che fare?

	C	A	R	V	E	R	S	Tot
	M	S	H	A	R	P	P	Tot
Asset 1	4	3	4	5	5	4	4	29
Asset 2	3	3	3	1	4	5	5	24
Asset 3	5	5	5	4	3	2	1	25

1) To decide that the whole target has the maximum value of those of each asset

2) Weigh through a multiplier value every single indicator depending on the strategic importance that the analyst wants to assign to that particular indicator

3) Make the average of the total value of the CARVER (S) indicators for each asset and the total number of assets

4) For each target / asset, scales are created to assign a numerical value to a risk band (Very high, High, Medium, Low, Very low)

CARVER(S) VS MSHARPP

- Decide to mitigate the risk:
  - reducing the criticality (backup systems, redundant systems);
  - reducing accessibility (implementation of physical security countermeasures);
  - reducing vulnerability (structural reinforcements, specific treatments);
  - reducing identification (erasing locations from maps, working on terrain conformations, planting vegetation).

- Performing analytical evaluations on each single result deriving from the methodologies (for example «vulnerability» and «criticality» may not have the same weight)
- In relation to the aims and the usefulness and the necessities, CARVER (S) from the "exterior looks inside" (outside looking in) while MSHARPP from the "inside looks out" (inside looking out): offensive purposes and defensive purposes.
- Change the indicators according to the context under analysis

CARVER(S) VS MSHARPP

$S = O * E * G$

$R = T * V * I$

Criticality	G	Mission	I
Accessibility	E	Symbolism	I
Recuperability	1/G	Historical	P=M*V
Vulnerability	O	Accessibility	V
Effect	G	Recognizability	I
Recognizability	O - E	Proximity	I
Shock	G	Population	I

Threat modelling (Electronic Frontier Foundation - https://ssd.eff.org)

1. What do you want to protect?
2. Who do you want to protect it from?
3. How likely is it that you will need to protect it?
4. How bad are the consequences if you fail?
5. How much trouble are you willing to go through in order to try to prevent those?

1. What do you want to protect? List of Risks
2. Who do you want to protect it from? Threats (natural or human)
3. How likely is it that you will need to protect it? P (T x V)
4. How bad are the consequences if you fail? I
5. How much trouble are you willing to go through in order to try to prevent those? Contermeasurements and residual risk

Conclusion 1/2

- In many cases, the risk assessment methodologies for CI are an adaptation of methodologies that have been used for assessing risks within the confined environment of an organization.
- These methodologies are tailored to the particular needs of this organization and biased to consider only part of relevant threats. In such context, the application is facilitated by the knowledge of architecture and functioning principles, which are the preconditions for modelling and subsequent simulation.
- This precondition is not always met when the risk assessment methodology exceeds the limits of the organization and aims at the assessment of systems of systems, such as interconnected infrastructure, for which the knowledge on architecture and functioning principles is fuzzy.
- The true challenge for upscaling any risk assessment methodology to complex systems is to develop effective approaches for the assessment of system of systems interdependences

Conclusion 2/2

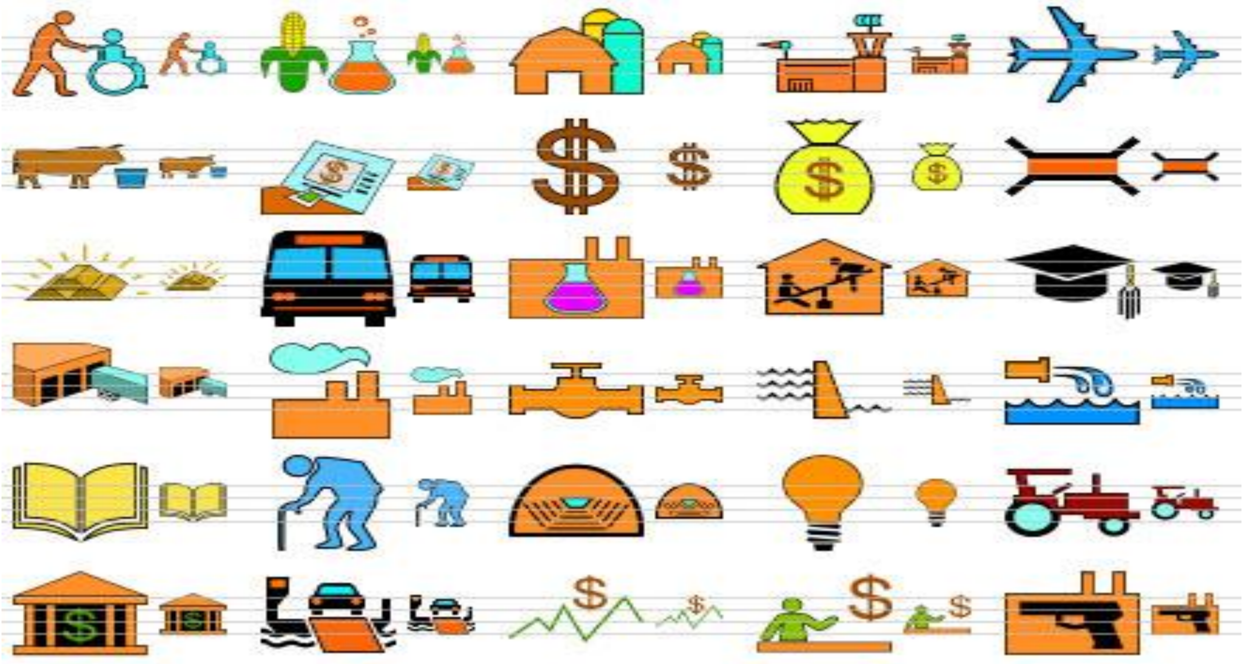
- The identification of a common methodology for cross-sectoral interdependencies evaluation would allow to assess cascading effects and return a common cross-sector risk figure so that comparison of sectors does not end up to a comparison of apples vs oranges.

- In order to define a common approach for interdependencies assessment further cooperation is required among government authorities, CI operators and stakeholders.

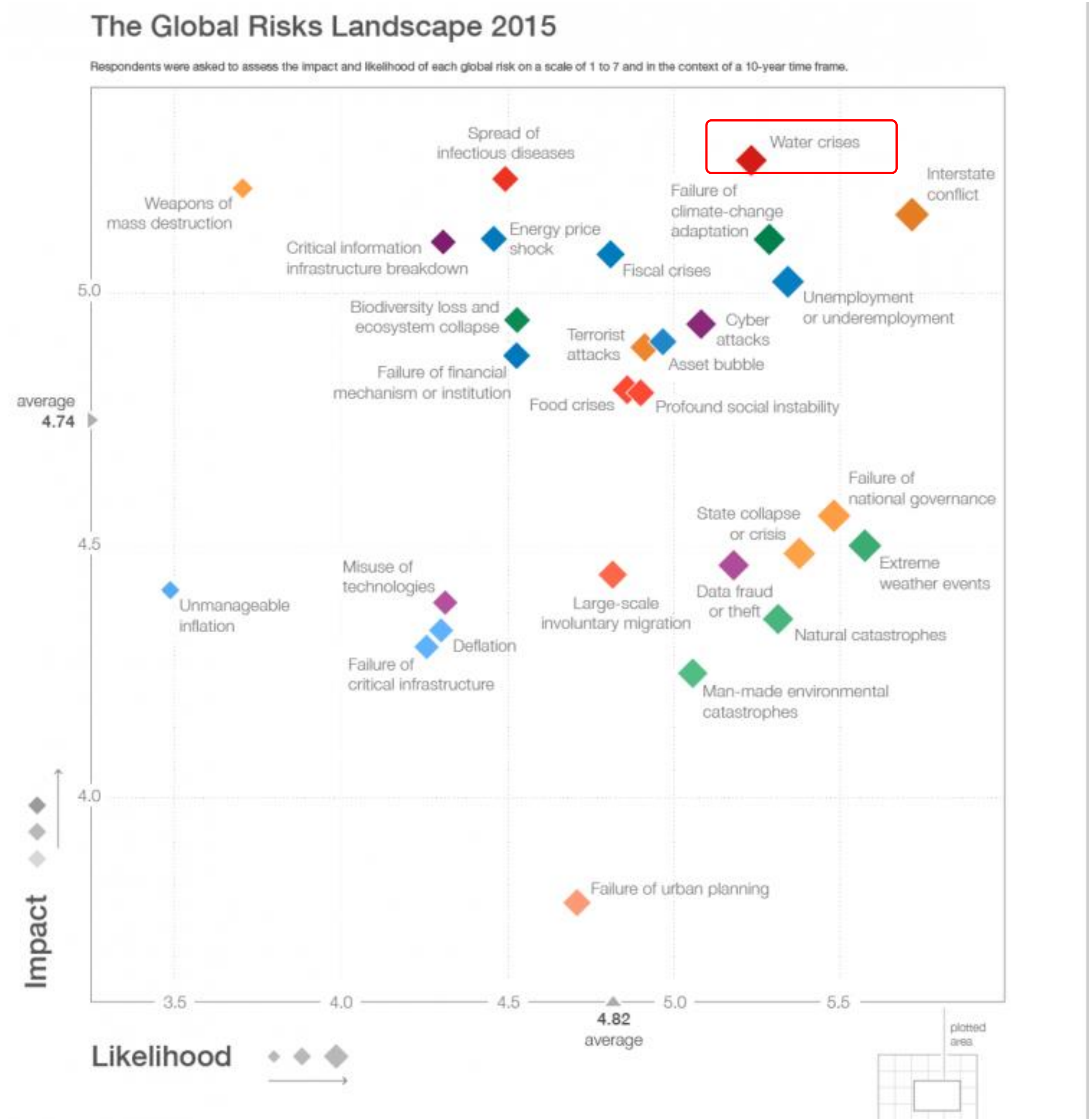
- Impact of infrastructure disruption is usually expressed in terms of aggregated figures that account for the economic losses. This is a straightforward choice that enables policy makers inter alia to evaluate different disruption scenarios including cascading effects across sectors and evaluate costs and benefits of mitigation measures.

- In all available methodologies, resilience seams to be the missing element, or in the best option it is only implicitly addressed.

Global risk report



The Risk Landscape

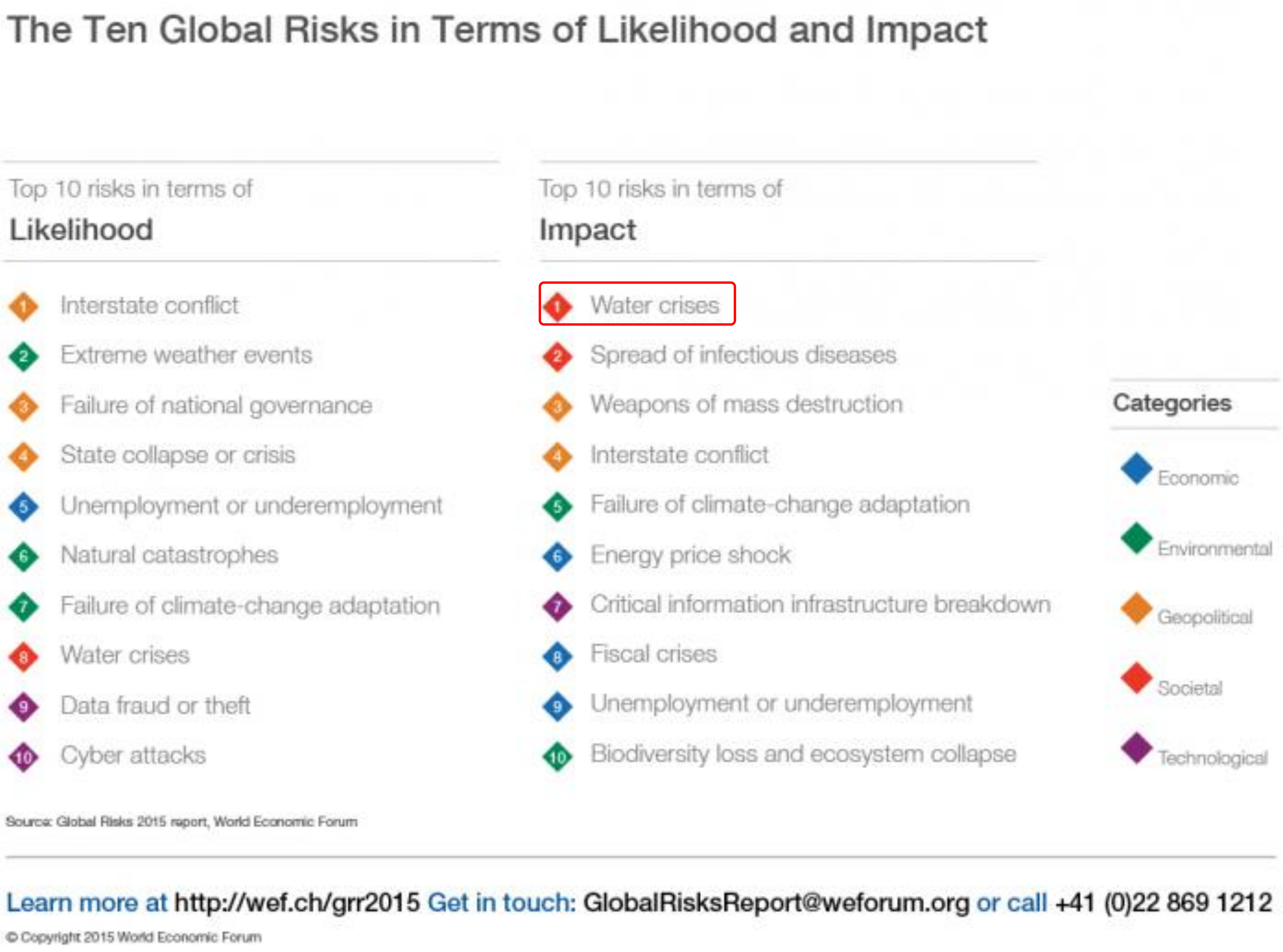


The Global Risks Landscape 2015

Respondents were asked to assess the impact and likelihood of each global risk on a scale of 1 to 7 and in the context of a 10-year time frame.

Fonte: *World Economic Forum - Global Risks Report 2015*

The Risk Landscape



The Ten Global Risks in Terms of Likelihood and Impact

Top 10 risks in terms of
Likelihood

1. Interstate conflict
2. Extreme weather events
3. Failure of national governance
4. State collapse or crisis
5. Unemployment or underemployment
6. Natural catastrophes
7. Failure of climate-change adaptation
8. Water crises
9. Data fraud or theft
10. Cyber attacks

Top 10 risks in terms of
Impact

1. Water crises
2. Spread of infectious diseases
3. Weapons of mass destruction
4. Interstate conflict
5. Failure of climate-change adaptation
6. Energy price shock
7. Critical information infrastructure breakdown
8. Fiscal crises
9. Unemployment or underemployment
10. Biodiversity loss and ecosystem collapse

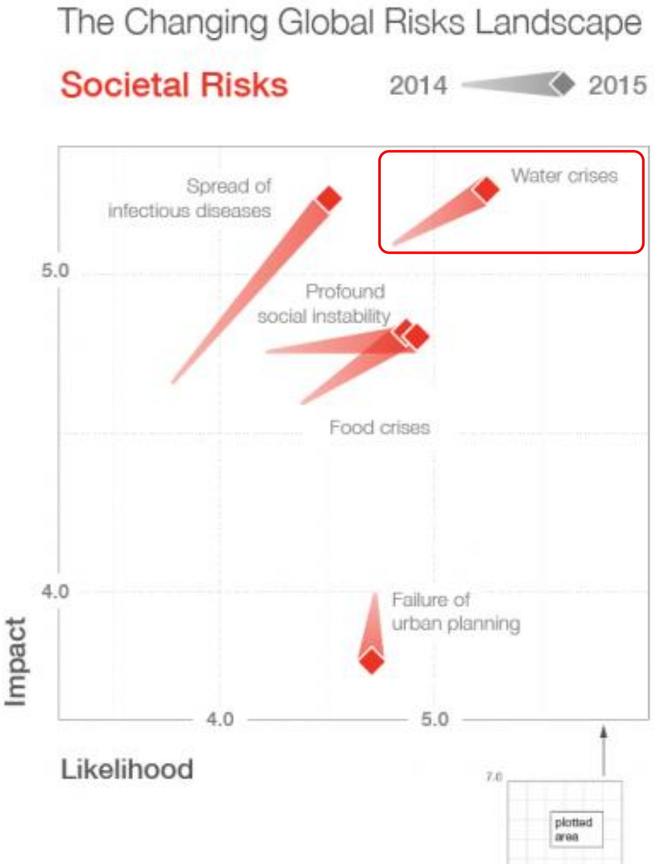
Categories

- ◆ Economic
- ◆ Environmental
- ◆ Geopolitical
- ◆ Societal
- ◆ Technological

Source: Global Risks 2015 report, World Economic Forum

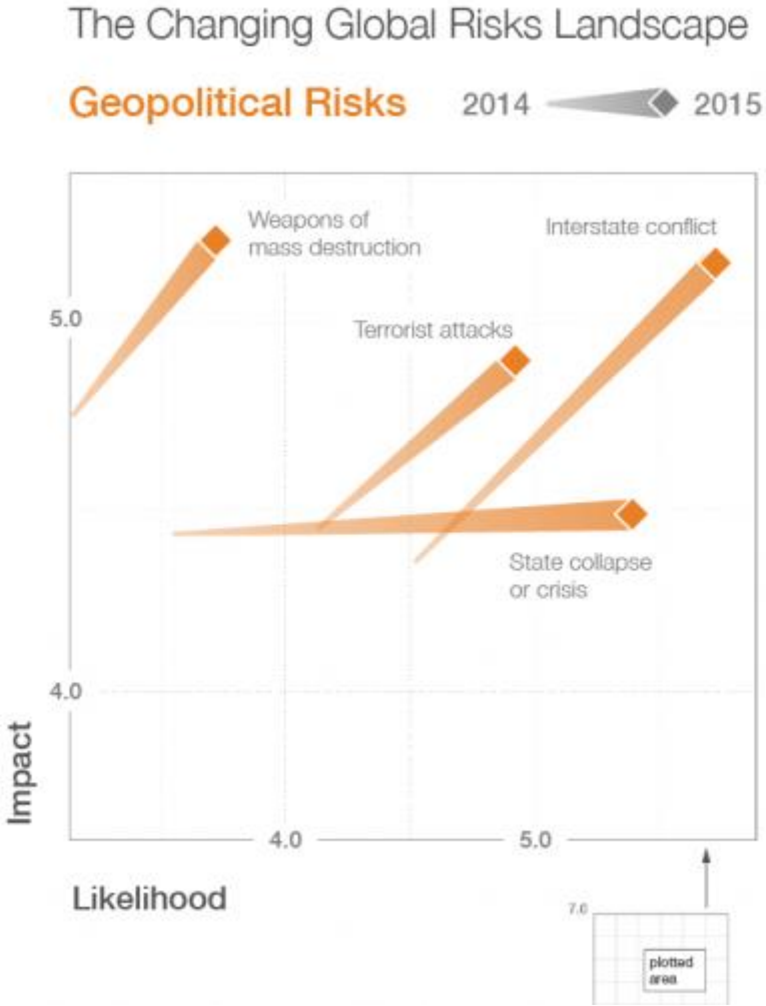
Learn more at http://wef.ch/grr2015 Get in touch: GlobalRisksReport@weforum.org or call +41 (0)22 869 1212

The Risk Landscape



The Changing Global Risks Landscape

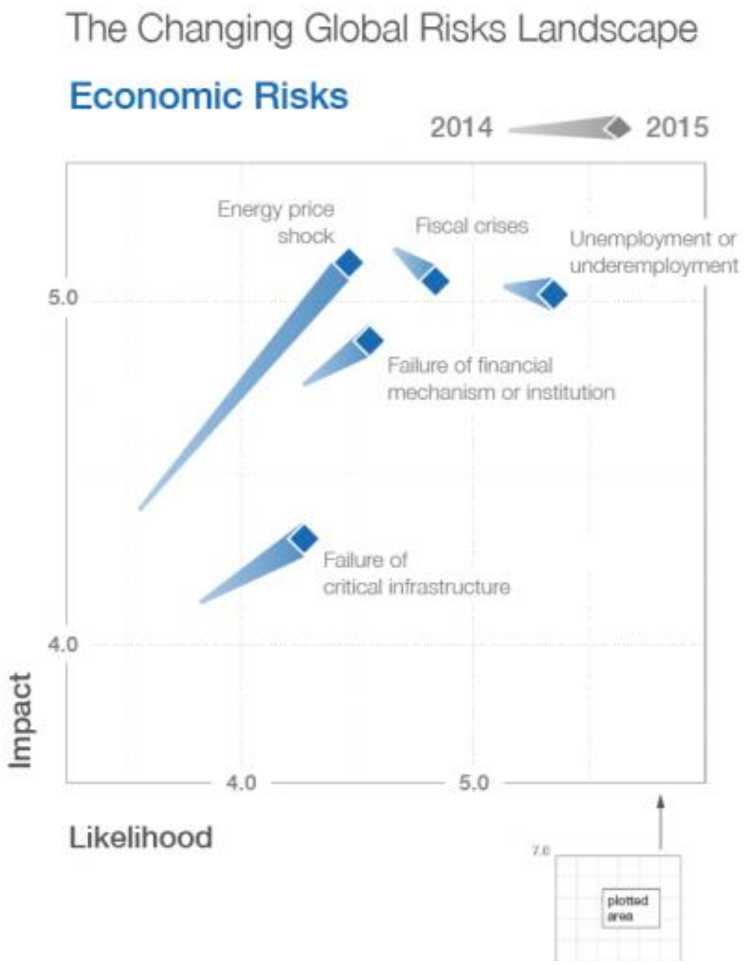
Societal Risks

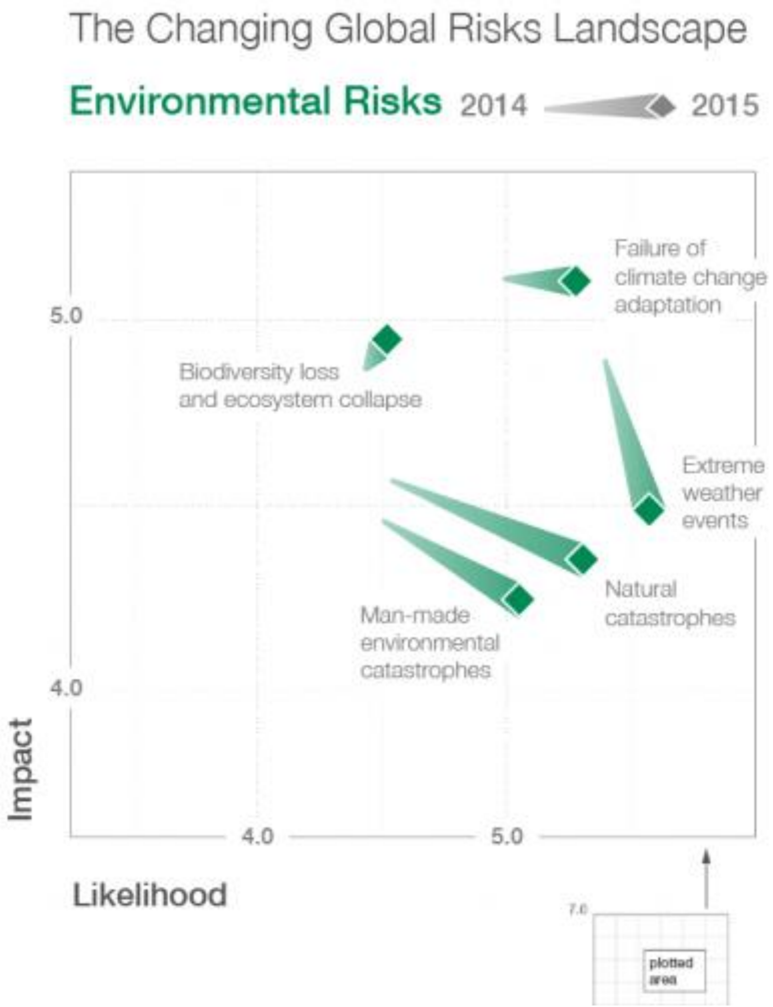


The Changing Global Risks Landscape

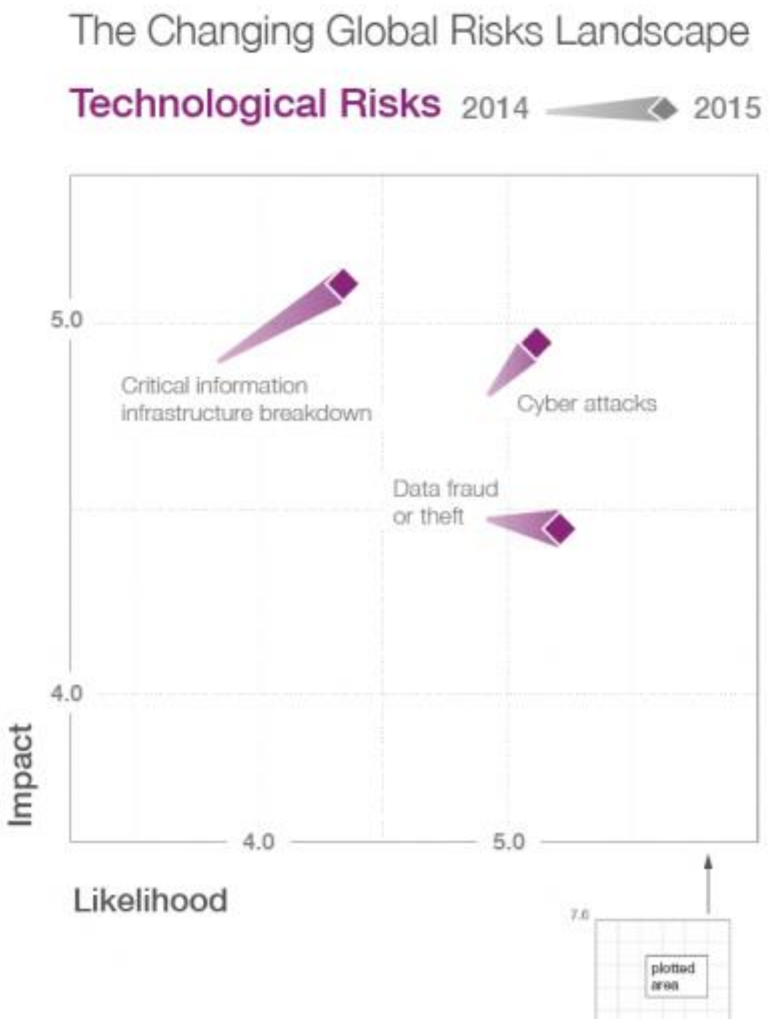
Geopolitical Risks

The Risk Landscape





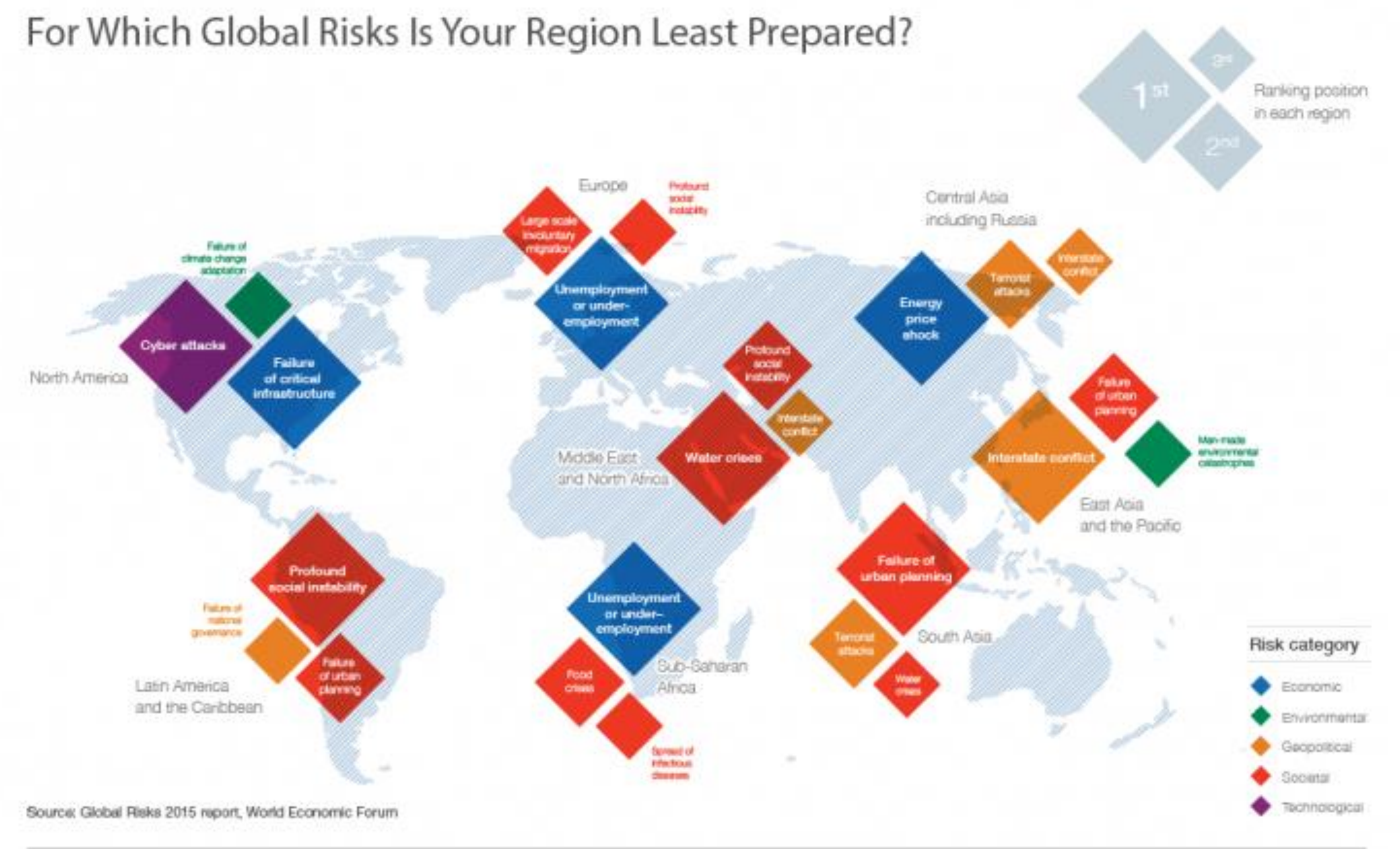
The Risk Landscape



The Changing Global Risks Landscape

Technological Risks 2014 2015

The Risk Landscape

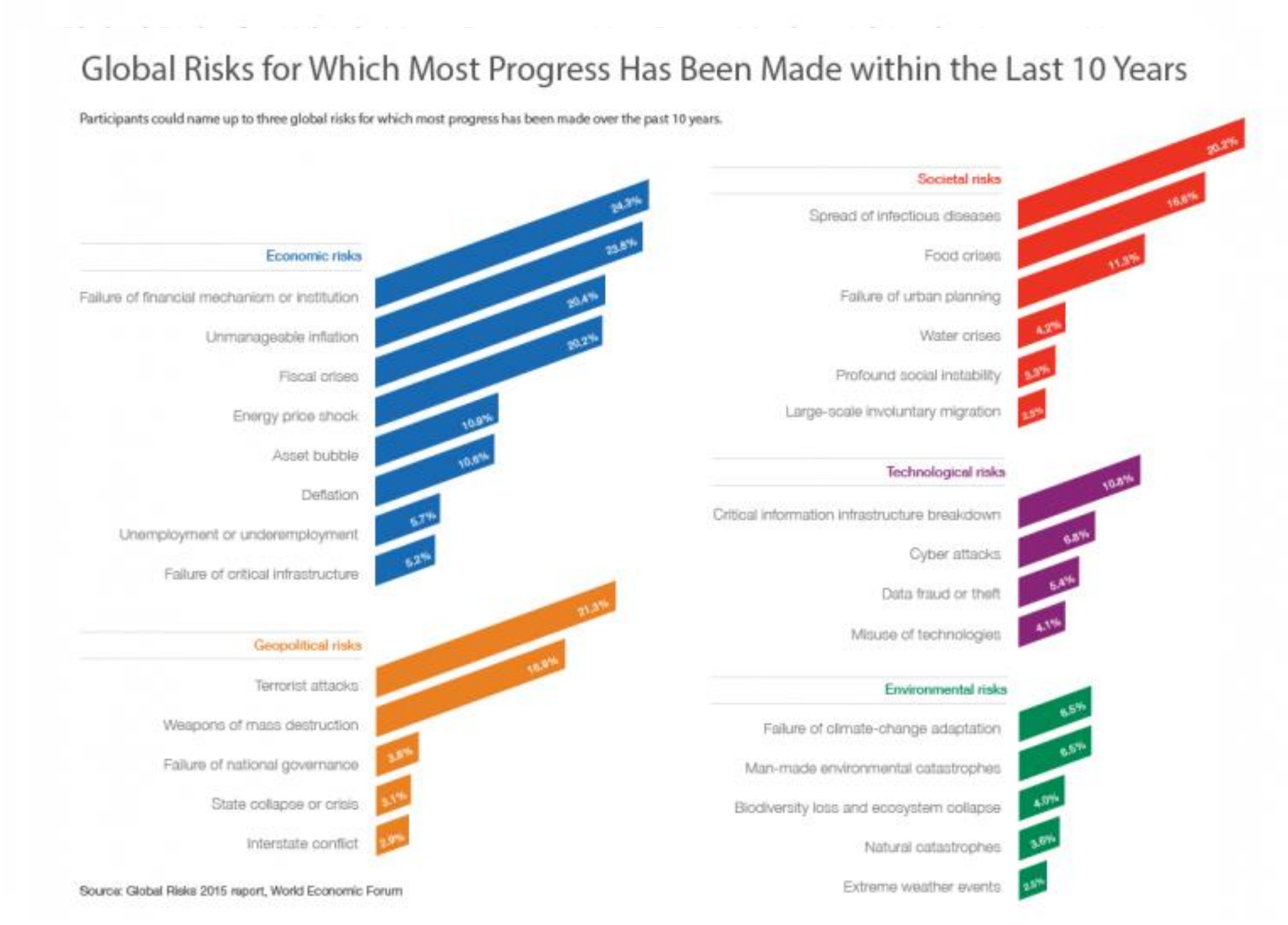


For Which Global Risks Is Your Region Least Prepared?

1st
2nd
3rd
Ranking position in each region
Europe
Large scale involuntary migration
Unemployment or under-employment
Profound social instability
North America
Cyber attacks
Failure of critical infrastructure
Failure of climate change adaptation
Central Asia including Russia
Energy price shock
Terrorist attacks
Interstate conflict
Middle East and North Africa
Water crises
Profound social instability
Interstate conflict
East Asia and the Pacific
Interstate conflict
Failure of urban planning
Man-made environmental catastrophes
Latin America and the Caribbean
Profound social instability
Failure of national governance
Failure of urban planning
Sub-Saharan Africa
Unemployment or under–employment
Food crises
Spread of infectious diseases
South Asia
Failure of urban planning
Terrorist attacks
Water crises
Risk category
Economic
Environmental
Geopolitical
Societal
Technological

Source: Global Risks 2015 report, World Economic Forum

The Risk Landscape



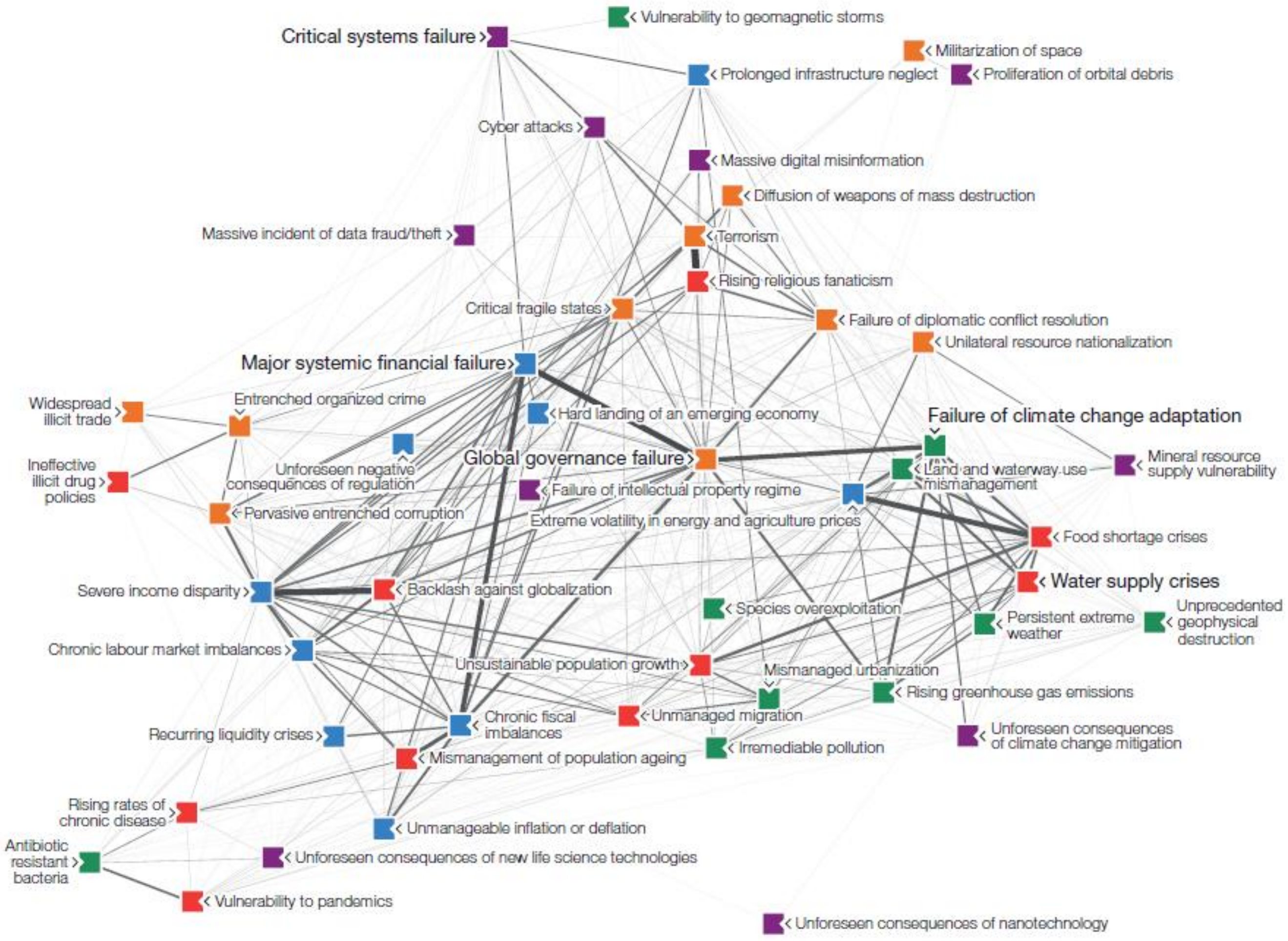
Global Risks for Which Most Progress Has Been Made within the Last 10 Years

Participants could name up to three global risks for which most progress has been made over the past 10 years.

Source: Global Risks 2015 report, World Economic Forum

The Risk Landscape

The Risk Interconnection Map 2013


Vulnerability to geomagnetic storms
Critical systems failure
Militarization of space
Prolonged infrastructure neglect
Proliferation of orbital debris
Cyber attacks
Massive digital misinformation
Diffusion of weapons of mass destruction
Massive incident of data fraud/theft
Terrorism
Rising religious fanaticism
Critical fragile states
Failure of diplomatic conflict resolution
Unilateral resource nationalization
Major systemic financial failure
Widespread illicit trade
Entrenched organized crime
Hard landing of an emerging economy
Failure of climate change adaptation
Global governance failure
Unforeseen negative consequences of regulation
Ineffective illicit drug policies
Land and waterway use mismanagement
Mineral resource supply vulnerability
Failure of intellectual property regime
Pervasive entrenched corruption
Extreme volatility in energy and agriculture prices
Food shortage crises
Severe income disparity
Backlash against globalization
Water supply crises
Species overexploitation
Persistent extreme weather
Unprecedented geophysical destruction
Chronic labour market imbalances
Unsustainable population growth
Mismanaged urbanization
Rising greenhouse gas emissions
Chronic fiscal imbalances
Unmanaged migration
Recurring liquidity crises
Unforeseen consequences of climate change mitigation
Mismanagement of population ageing
Irremediable pollution
Rising rates of chronic disease
Unmanageable inflation or deflation
Antibiotic resistant bacteria
Unforeseen consequences of new life science technologies
Vulnerability to pandemics
Unforeseen consequences of nanotechnology

Fonte: *World Economic Forum - Global Risks Report 2013*

luisa.franchina@libero.it