WP 3: Urban public transport

SOCIO-ECONOMICS MEETS SECURITY

UITP SecCom
Karlsruhe 17-2-2014

Content

1. Brief Remainder
2. Scenarios Summary
3. Societal model
4. Risk Analysis model
5. Open discussion

1.- Brief Remaider

SECONOMICS goal is **synthesizing sociological**, **economic and security science** into a usable, concrete, actionable knowledge for policy makers and social planners responsible for citizen's security.

Main Objective: To contribute with the public transport (underground) requirements to develop SECONOMIC framework, which will comprise a set of methodologies and techniques produced in WP4, 5 and 6 and the development of a security decision-making tool in WP8.

This main objective is broken down in sub-objectives

1. Identification and analysis of underground transport requirements and security challenges.

2. Validate the methods, techniques and models developed in WP4, WP5 and WP6.

3. Evaluate the security policy decision making tool.

SECONOMICS
Socio-economics meets Security

Threat | Asset

Risk

Vunerability
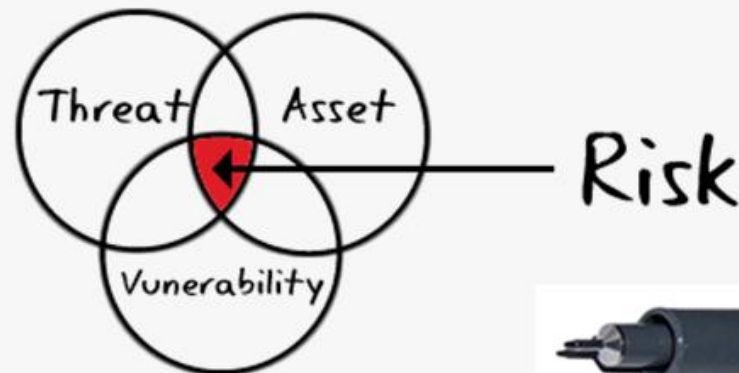
2.- Scenarios Summary

The project focuses on the impact of security measures applied by public transport operators.

For that it has been chosen scenarios and incidents affecting, **directly or indirectly**, the **sense of security and the objective security**. Those types of security incidents also have a direct impact on customers and / or service.

The selected scenarios in the area of public transport are:

- Indicators of economic crisis
- Fraud
- Graffiti
- Pickpockets

Refinement of motivations

– **Uncivic behaviour**: Individual and / or sporadic behaviour not adjusted to socially accepted code of conduct, which causes a state of uneasiness and discomfort in people who witness it.

– **Antisocial behaviour**: Behaviour of an organized nature and / or intentional or recidivist involving violations of criminal or administrative regulations with a clear social disdain.

– **Criminal behaviour**: Behaviour defined in the criminal laws in force.

Other interesting scenarios are not taken into account, since the public transport operators will affect relatively:

- Terrorism:
  - To combat it, intelligence tools are needed
  - There is a close collaboration with the security forces (sniffer dogs, access to CCTV recordings)
  - Metro facilities are an extension of the public space
  - Accessibility and massive nature in this type of public transport has priority

- Security threats in information systems
  - Exclusive control systems railway sector
  - Communications of these systems are done with close communications infrastructure

A. Indicators of social and / or economic crisis (I)

With the crisis, it has been detected an increase of anti-social incidents affecting the security perception of the users

- Musicians
- Sleepers
- Beggars
- Hawkers

A. Indicators of social and / or economic crisis (II)

- *Typology:*
  - Uncivic behaviour, on an individual basis
  - Antisocial behaviour, when the activities are carried with some degree of organization, which have a higher impact.

- *Treatments:*
  - Individuals, they are accompanied outside the facilities
  - Organized, they deserve administrative or criminal complaints (for organized hawking of intellectual property)

- *Impact:*
  - Economic impact is low
  - Social impact is low for individuals, and medium to high for the organized activities

Typology	Uncivic	Antisocial	Criminal
Musicians	YES	-	-
Organized musicians	YES	YES	-
Sleepers	YES	-	-
Beggars	YES	-	-
Organized beggars	YES	YES	-
Single hawking	YES	-	-
Organized hawking	YES	YES	-

B: Fraud (I)

The activities of fraud and counterfeiting have two causes:

- Activity of <u>organized groups</u> with protest purposes, such as collective and inductive fraud

- For economic reasons

The <u>number of individual incidents has decreased</u> due to the economic crises- the total number of passengers has also decreased, and also thanks to new strategies for the tickets inspection.

<u>Collective and inductive activities</u> have increased because of the activity of some organized groups with protest purposes.

SECONOMICS

B: Fraud (II)

- *Typology*:
  - Uncivic, tickets not paid without disturbing nor promoting this among other users
  - Antisocial, recurrent or affect other users, including collective and organized
  - Criminal, when committing fraud due to counterfeit

- *Treatments*:
  - Individual and multiple offenders, information campaigns to promote good behaviours, strategic placement of security guards
  - Massive fraud, avoid appearing in the media, adjusting the resources allocated
  - Counterfeit, material control and inclusion of additional safety measures in the tickets

- *Impact*:
  - The highest economic impact are scams and fakes of tickets
  - The highest social impact is caused by subgroups with protest and vindictive purposes

Typology	Uncivic	Antisocial	Criminal
Individual	YES	-	-
Multiple offender	-	YES	-
Collective and organized	-	YES	-
Inductive	-	YES	-
Scam / counterfeiting for profit	-	-	YES
Scam / counterfeiting for vindictive purpose	-	YES	YES

13

C: Graffiti (I)

Usually graffiti is part of what is generally known as vandalism, so this was chosen as its greatest exponent, both for its economic impact and the amount of resources devoted to its management.

Currently the most frequent graffiters are <u>organized into groups</u>, have <u>technical and operational elements</u>, and use some <u>criminal techniques and procedures</u> to achieve their objectives. The main aim of this activity is to display, distribute and exhibit their achievements on the Internet and social networks.

C: Grafiti (II)

- *Typology*:
  - Uncivic, done by individuals in single colour, usually corresponding to "signatures"
  - Antisocial, performed with premeditation, by multiple offenders, in a collective and organized way, usually on parked trains, and eventually with passengers on-board
  - Criminal, an amendment of the Spanish criminal law in 2010, stopped graffiti to be considered a crime or damage. Now it is more difficult to act effectively against this phenomenon in the courts.

- *Treatments*:
  - Remove graffiti painted trains from service, to avoid promotion / dissemination of their "work", and to proceed with their cleaning.

- *Impact*:
  - The economic impact is considered very high, particularly for the wall graffiti. Impact on the QoS
  - The social impact is not as high as it should

Typology	Uncivic	Antisocial	Criminal
Individual	YES	-	-
Multiple offender	-	YES	-
Collective and organized	-	YES	-
With passengers on-board	-	YES	-

D: Pickpockets (I)

The phenomenon of pickpockets is also a recurring problem in rail transport, with different quantitative and qualitative intensity, and, as noted before is a concern in many subways worldwide

In the case of Barcelona, it is a problem inherent to the city, since many variables influence the phenomenon:

- Criminal and procedural regulation is more rights-based in Spain than in other countries of southern Europe.

- The application of existing regulation is not entirely effective in the courts

- The city of Barcelona is a touristic destination

In the Metro,
be extra careful in crowds.

16

D: Pickpockets (II)

- *Typology*:
  - Uncivic, notice of presence at stations or trains of people normally identified as pickpockets
  - Criminal, carelessness thefts that corresponds to a criminal who works isolated and on an individual basis and theft by "organized groups", performed by groups between three and ten organized pickpockets

- *Treatments*:
  - When a pickpockets announcement is made it is only possible to invite them to go out
  - Information and communication campaigns, especially in stations frequented by tourists
  - Reducing the overcrowding with the Increase of trains frequency or improving spaces
  - Through the on-going dissemination of instructional videos with advices to potential victims
  - Through deterrence by the presence of personnel in hot spots of the Metro network

- *Impact*:
  - The economic impact is considered very low for the operator
  - The social impact is medium to high, especially when the levels of criminal activity of this phenomenon are high and it becomes present in the media

Typology	Uncivic	Antisocial	Criminal
Pickpockets announcements	YES	-	-
Thefts due to carelessness	-	-	YES
Thefts by organized groups	-	-	YES

17

- **Uncivic behaviour**: The most common that affect the subway service. The most relevant is to interpret their evolution and the degree of citizens' acceptance /rejection towards them.

- **Antisocial behaviour**: Of particular concern is the increase in violence, particularly in groups close to the anti-system ideologies.
  - Graffiti: traditionally nonviolent, now cause assaults and serious damages. The use of internet and social networks allows publication of their "works" spreading this "fashion".
  - Proliferation of organizations that attempt to promote fraud practices through various techniques that do not detract from the objective, which is to fight the operation and financing of public transport system.
  - International criminal networks As with some of the antisocial acts (e.g., graffiti), cross-border activities are a note of paramount importance.
  - The arrival of other emerging criminal actions is not expected, except those coming from consolidated antisocial acts (massive fraud, tickets scams...)

SECONOMICS

- To have a scalable and configurable model for different operators of underground public transport for security risk planning and social models of security

- Selected scenarios correspond to safety problems, emerging or existing, which become important because of changes in society

Selected scenarios	Security and society (WP4)	Security risk models (WP5)
Impact of new security measures (automatic doors generate personal conflicts)	✔	
Civil disobedience, promoting not to pay (using internet social platforms)	✔	
Promotion of producing fake tickets (tutorials available in the internet)	✔	
Individual fare evaders		✔
Colluding fare evaders (using actively social networks)		✔
Organised pickpocketing (tourists wanted)		✔

3.- Security and society: Societal Model

SECONOMICS

Security has been defined as a subjective phenomenon that changes within society. Information on people's understanding of security issues (e. g. crime, terrorism, natural or man-made disasters), their perception of security as well as the relevant facts about the risks and dangers they face, and perceive may vary according to the level of assessment, be it public or personal (individual).

Furthermore, people's feelings of insecurity and their perception of the importance of security can be different in diverse demographic groups. Persons who are amongst best protected and most secure in the society are likely to have expectations of security much higher than poorer, less protected persons.

Seconomics project seeks to tackle the following questions:

- How do media actually frame the implications of security and security technologies within the three SECONOMICS case studies?

- What are the perceived trade-offs between security and privacy? Do questions of security dominate? Who are the proponents and opponents of security vs. freedom (privacy)?

- Has the media coverage of terrorism made the public more sensitive to the issue of security? And, if so, how are the (security) threats perceived and discussed by the media?

- What is the role of social media in shaping public opinion and framing security dilemmas?

- Do new technologies offer some answers to security issues, or do they represent new risks?

SECONOMICS

Graph 1. Publically perceived major problems in Spain (2007-2012)
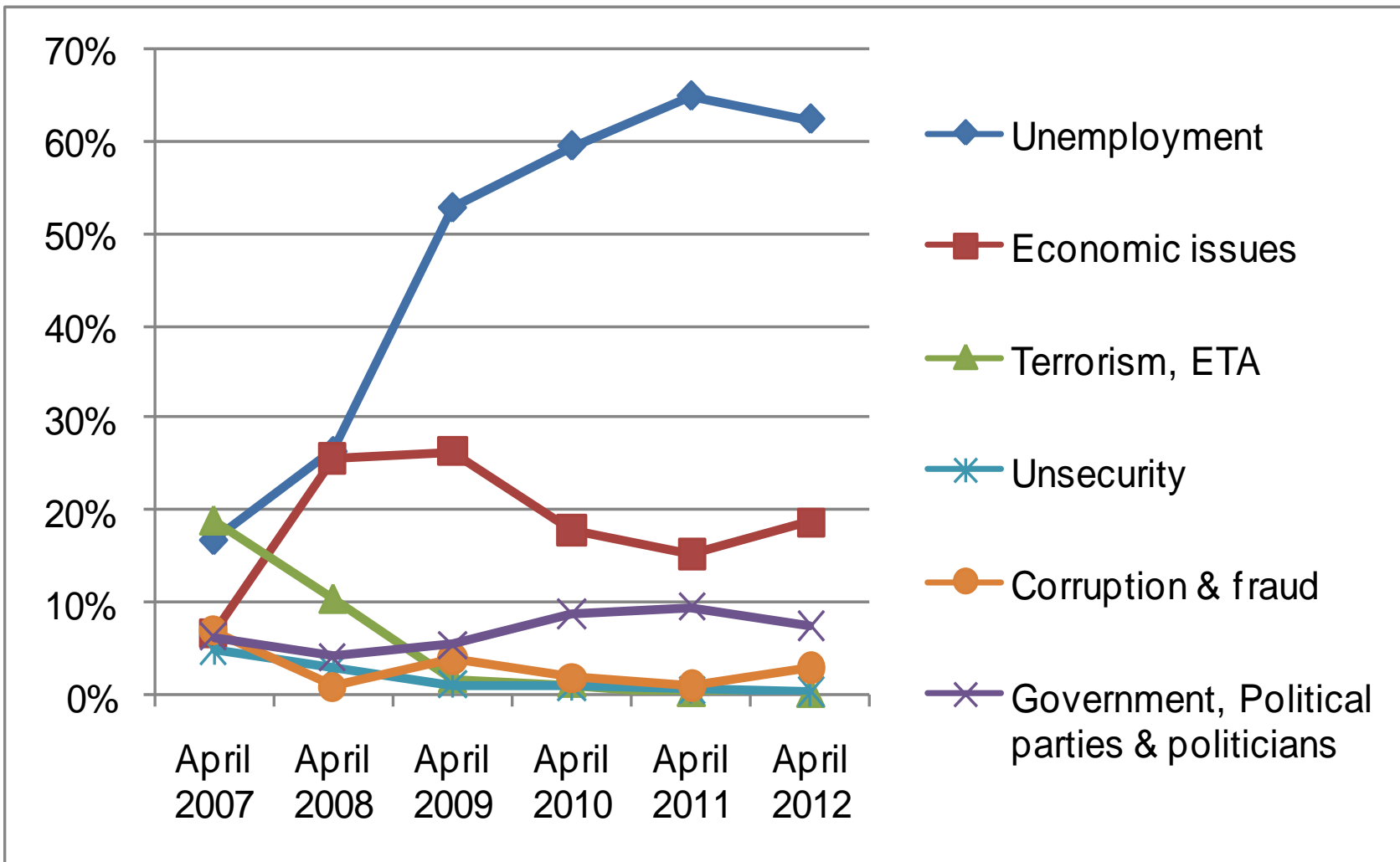
Source: *Centro de Investigaciones Sociológicas* (CIS)

SECONOMICS

In order to gain better understanding of salience and acceptance of security measures related to public transport ISASCR and TMB in collaboration analyzed following data:

(1.) media articles from two Spanish newspapers from 2010-2013 (focusing on three security issues - 3D body scanner, CCTV cameras and Stuxnet);

(2.) security data of TMB on incidents in metro (2011-2013, categorized by security issues);

(3.) passenger complaints data (2011-2013), categorized by security issues.

Defining Salience

→ For the purpose of this study, salience is defined as public perception and reception of security issues and more particularly of security measures; for this purpose salience signifies the degree of acceptance (positive salience) and the degree of rejection (negative salience).

SECONOMICS

- Our study analyzed the coverage of two Spanish major newspapers on three highly relevant topics affecting security: implementation of 3D body scanners, the use of CCTV systems and the release and consequences of the IT virus called *Stuxnet* in the period from January 2010 to April 2013;

- here we will concentrate on the CCTV camera issue; because they seem to be the most relevant for Metro;

- from the total amount of the chosen 172 news articles, 41 were selected to be analyzed (around 25% of the total number, N), keeping the proportion of articles published by media, topic and year.

Table 1. Articles on *3D body scanners*, *Stuxnet* and *CCTV* published by *El País* and *La Vanguardia* 2010-2013

		2010	2011	2012	2013	Total
EL PAÍS	3D body scanner	31	3	4	1	39
	stuxnet	15	17	11	2	45
	cctv	13	7	6	0	26
LA VANGUARDIA	3D body scanner	9	0	0	0	9
	stuxnet	6	3	3	0	12
	cctv	14	15	9	3	41
Total		88	45	33	6	172

Source: ISASCR

SECONOMICS

- State institutions including the Catalonian data protection agency, the Madrid-based commission of surveillance, as well as city councils are quoted many times by journalists to provide information on the installation of new CCTV cameras in public places;

- citizens support CCTV systems as a good measure to fight against petty crimes and daily criminality, nevertheless, it could be suspected that Spanish media try to hide citizen critics towards this technology;

- most of the actors quoted support the implementation of video-surveillance;

- stakeholders consider that video-surveillance can be a good strategy to face threats such as burglary or vandalism; however, they hardly mention terrorism as one of the potential risks.
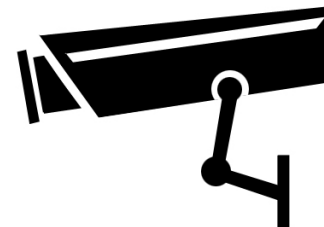
- CCTV salient in positive way, especially in Catalonia, highly accepted crime-prevention measure;

- Overall we find low negative salience (complains) - especially of the uncivic behavior and fare evasion, and medium negative salience of the TI's behavior;

- Over time the importance of the negative salience of the uncivic behavior and of the TI's behavior is growing;

- In order to decrease passenger satisfaction & reduce negative salience among the issues analyzed, TI training is a possible issue;

- High level of correlation between incidents and complains over time, hints to the fact that in-depth qualitative analysis of complaints can provide an important insights into issues of passenger's (security-related) concerns.

From January 2011 to June 2013 TMB detected **19.606** incidents of which **9.599** have connection to fare evasion.

That means a 48.96%,

These were:

1. Uncivic behaviour (18.81%)
2. Assaults (25.78%)
3. Screen access doors broken (56.98%)
4. Threats (32.07%)

Another source of information, qualitative one, which we worked with are passenger complaints – from January 2011 to June 2013 TMB received **9883 complaints** (growth over time);

Combining these data allows us to yield new information about passenger perception of security measures.

SECONOMICS

The Relationship between reported cases and complaints 2011-2013 TMB

Source: Data TMB, analysis IS AS CR

SECONOMICS
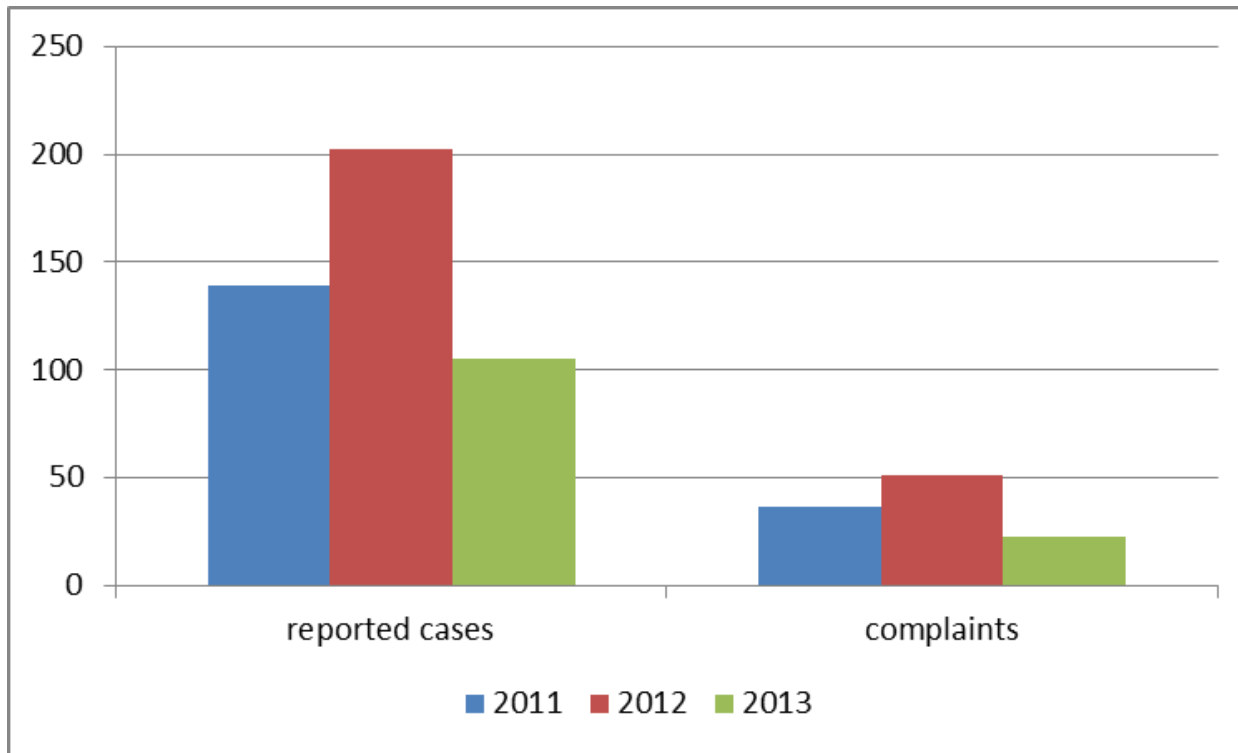
Overview of overall complaints per month 2011-2013 TMB
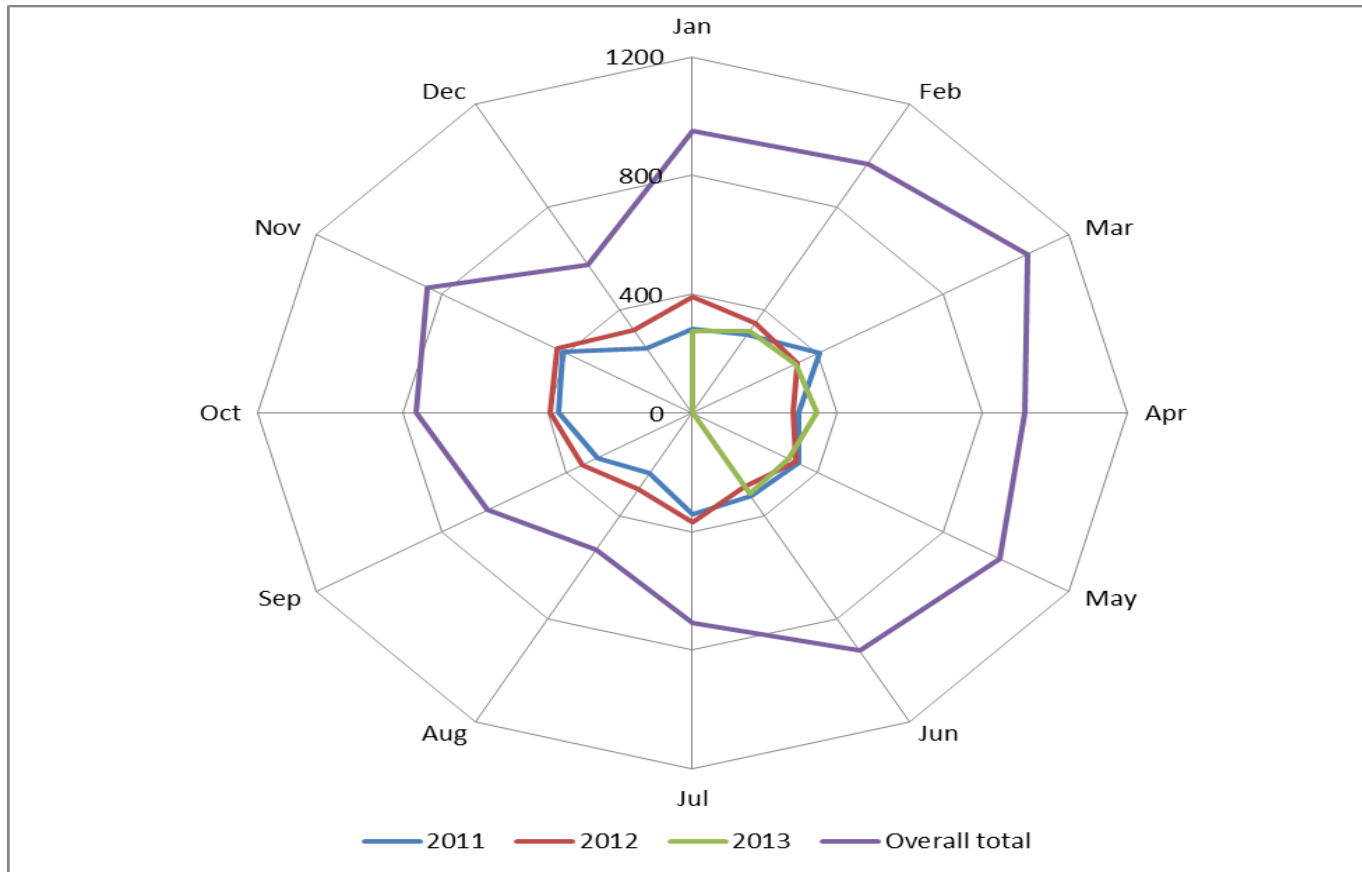
Source: Data TMB, analysis IS AS CR
N=9883

Comparison of selected complaints per month 2011-2013 TMB

Uncivic behaviour of other passengers
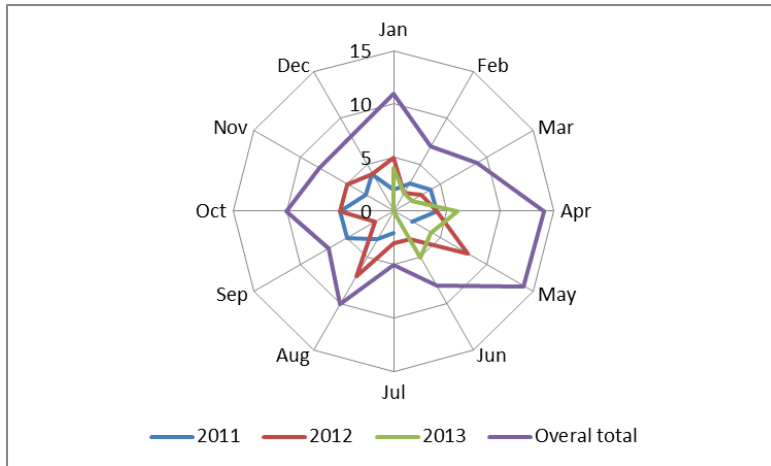
Ticket inspector behaviour

Fare evasion

Source: Data TMB, analysis IS AS CR

SECONOMICS
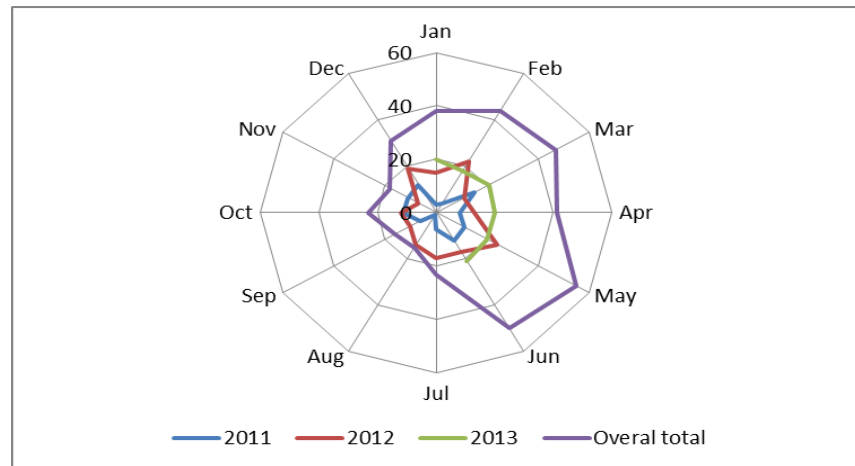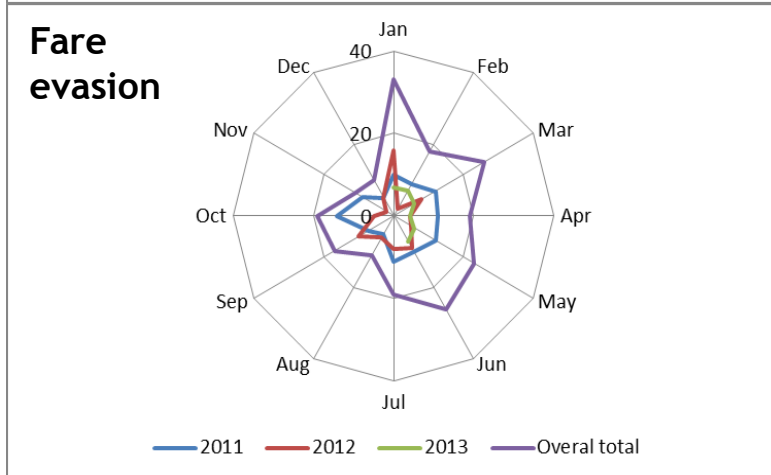
Critical Salience of selected security issues over time TMB

Source: data TMB, analysis IS AS CR

SECONOMICS
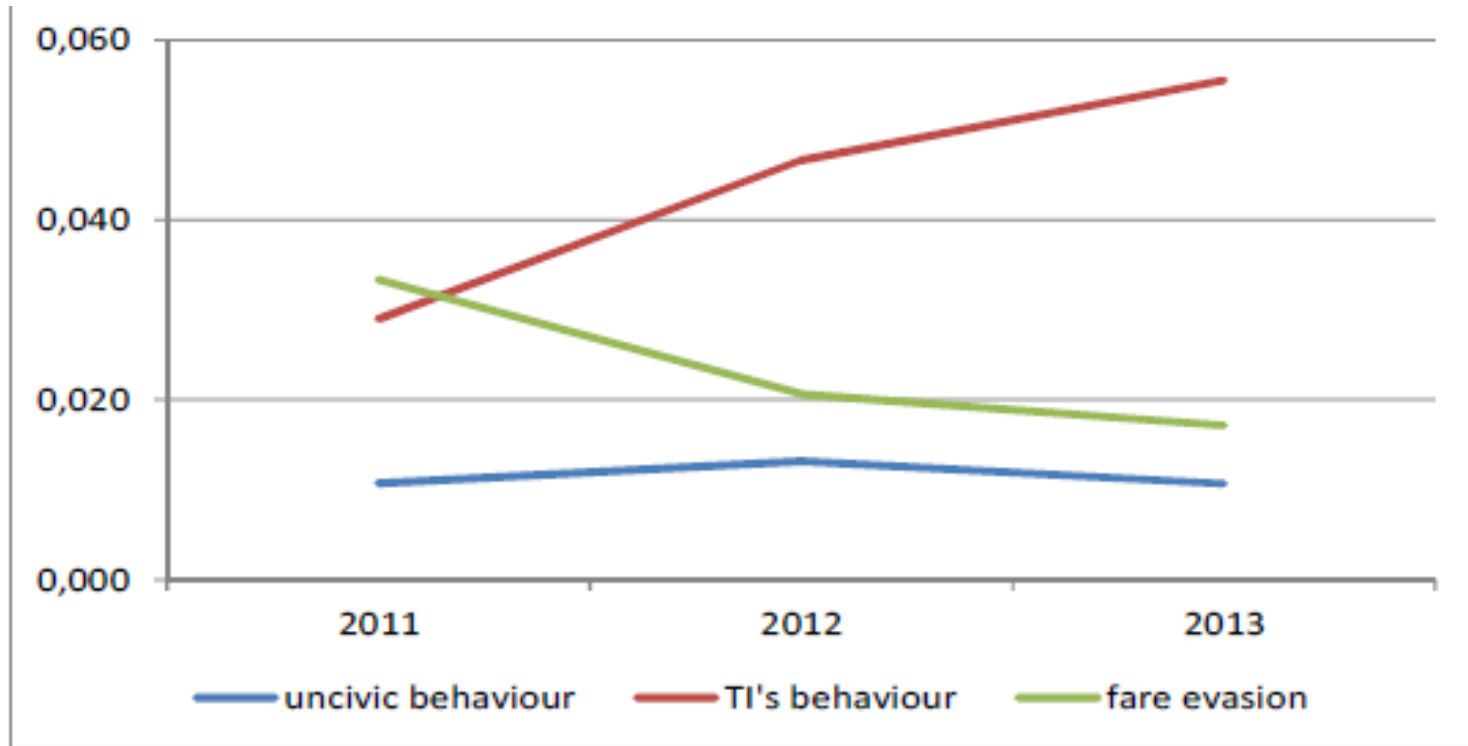
1. Based on TMB assessment, the effect of HR resources on customer satisfaction varies – Guard with dog less accepted than single guard (i.e. rather negative/low, according the experience from TMB staff).

2. As for technical resources, the initial TMB assessment is as follows - CCTV cameras (acceptance neutral/high), this was further confirmed by WP4 media analysis for both Spanish and especially Catalan newspapers.

3. As for Ticket-validation-gates– the level of acceptance is low (due to novelty, and new forms of fare evasion including inhibiting personal space of paying customer by fare evader).

1. CCTV salient in positive way, especially in Catalonia, highly accepted crime-prevention measure;

2. Overall we find low negative salience (complains) - especially of the uncivic behaviour and fare evasion, and medium negative salience of the TI's behaviour;

3. Over time the importance of the negative salience of the uncivic behaviour and of the TI's behaviour is growing;

4. In order to decrease passenger satisfaction & reduce negative salience among the issues analyzed, TI training is a possible issue;

5. High level of correlation between incidents and complains over time, hints to the fact that in-depth qualitative analysis of complaints can provide an important insights into issues of passenger's (security-related) concerns.

4.- Security risk model

SECONOMICS

- To provide a set of template models for risk analysis for critical infrastructure protection, helping to assess the most effective countermeasures.

- To adapt them to the case studies developed.

- Based on the gained experience, to describe a general methodology for risk analysis for critical infrastructure protection.

- To describe a computational tool supporting the proposed methodology.

SECONOMICS

- **Risk Analysis:** methodology to mitigate the negative effects of threats that may harm the performance of a system.
  - Eg: hurricane, earthquake, ...

- **Adversarial risk analysis** expands the methodology focusing on threats coming from **intelligent intentional adversaries**
  - Eg: terrorism, smuggling, ...

- Advises the defender against threats of intelligent attackers.

    – It is based on a **subjective model with multiple objectives**.

    – Attacker's **random decisions.**

    – Attacker's **preferences** are evaluated

    – It is assumed that the attacker tries to **maximize** its benefits / rewards

- Sequential Defend-Attack Model
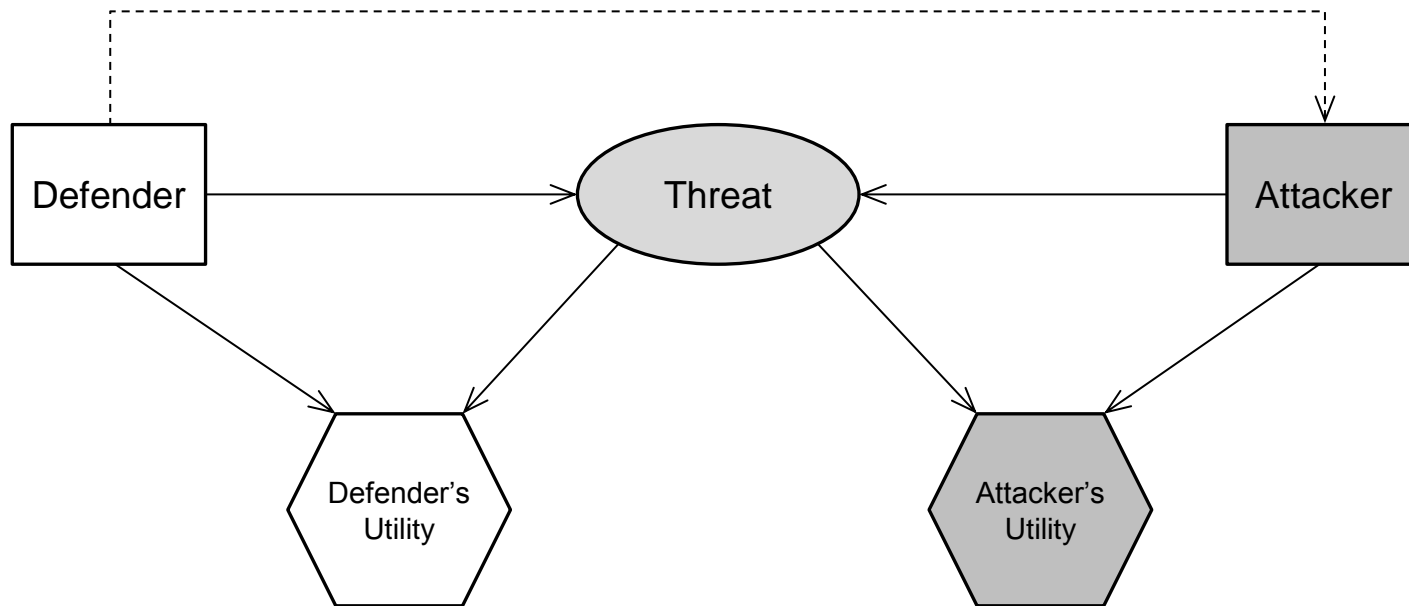
SECONOMICS

| One threat. | Fare evasion One station | Standard evaders Colluders Standard+colluders |

| Two threats. | Fare evasion Pickpocketing by a team |

Extension to more than one station

SECONOMICS
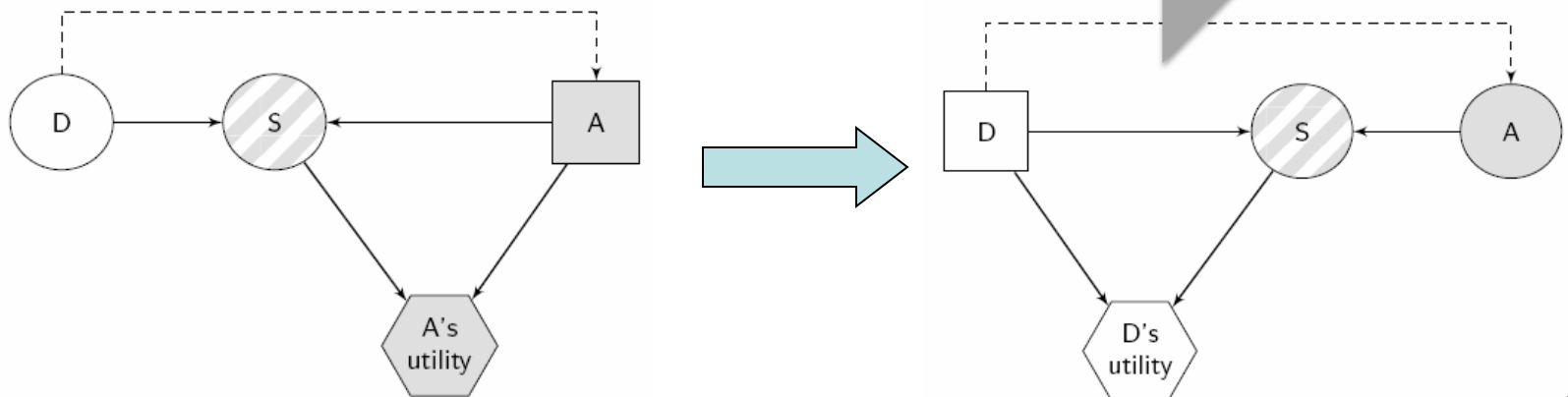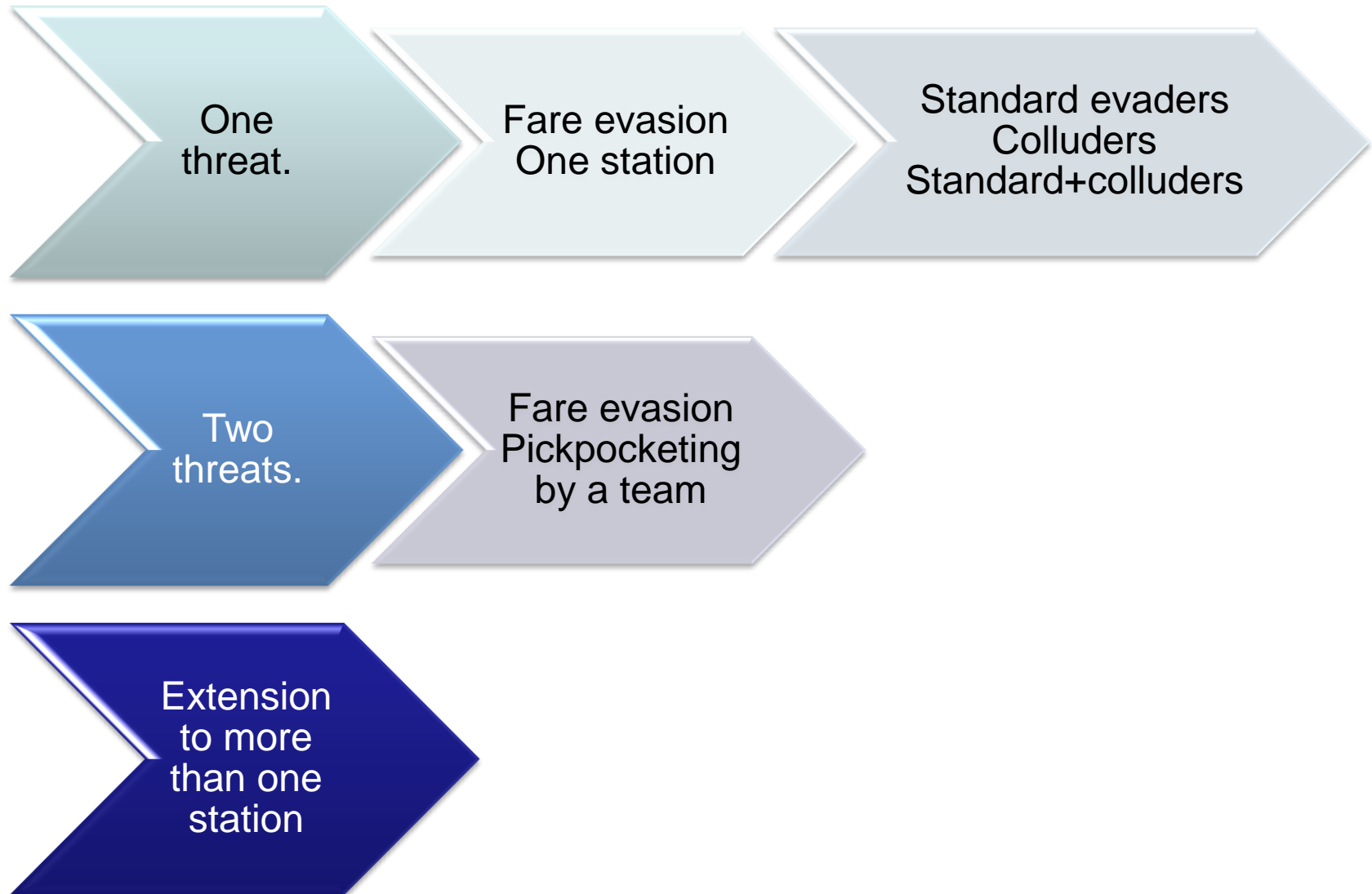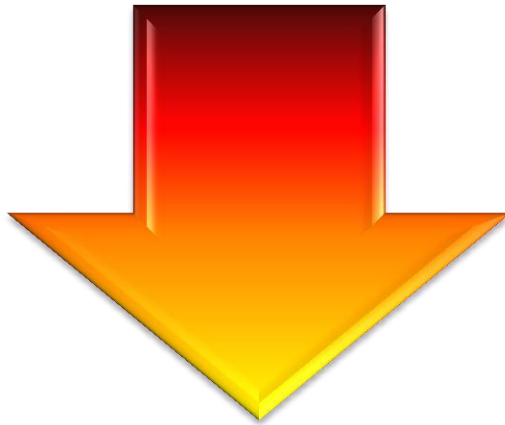
Two types of evaders:

- Standard (standard random process).
- Colluders (ARA; explicitly modeling intentionality).

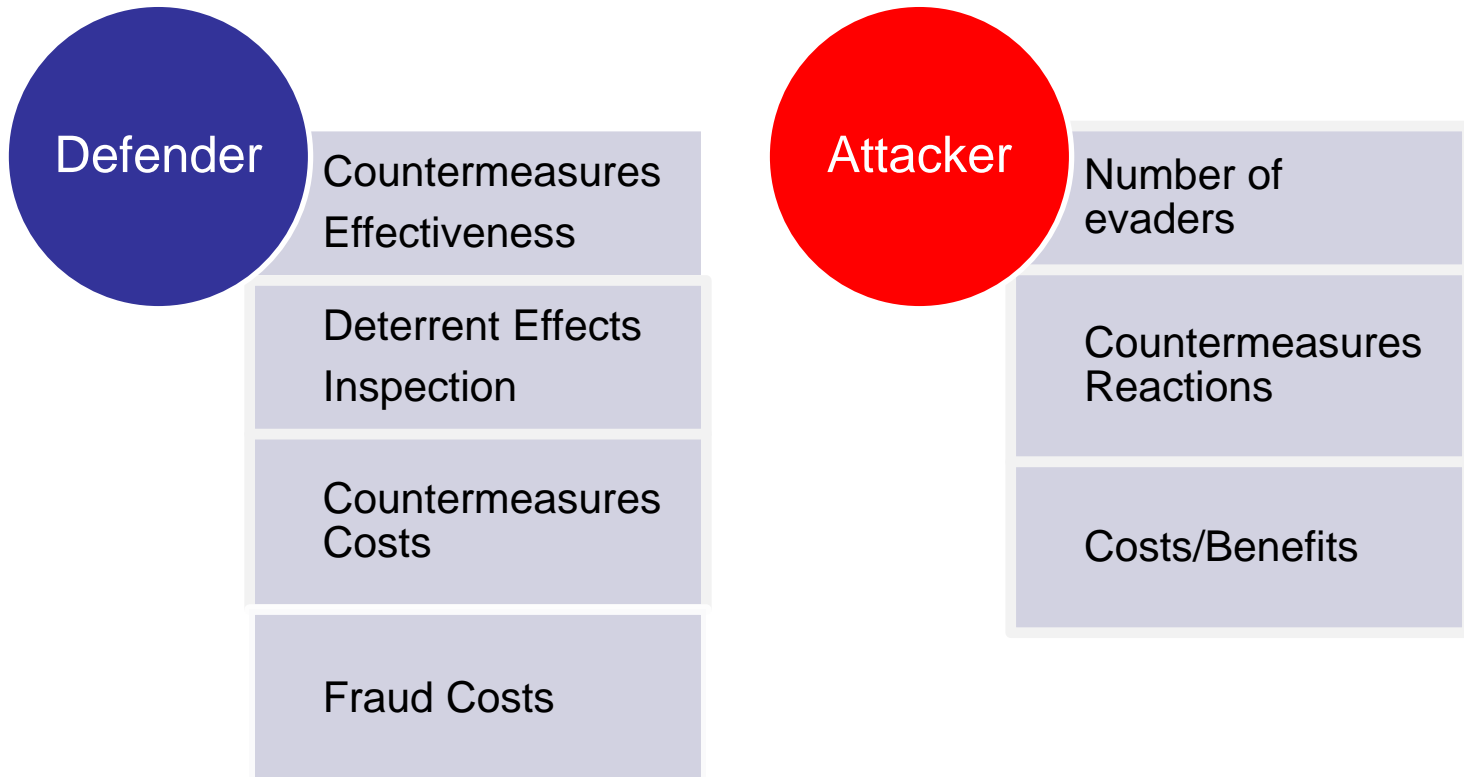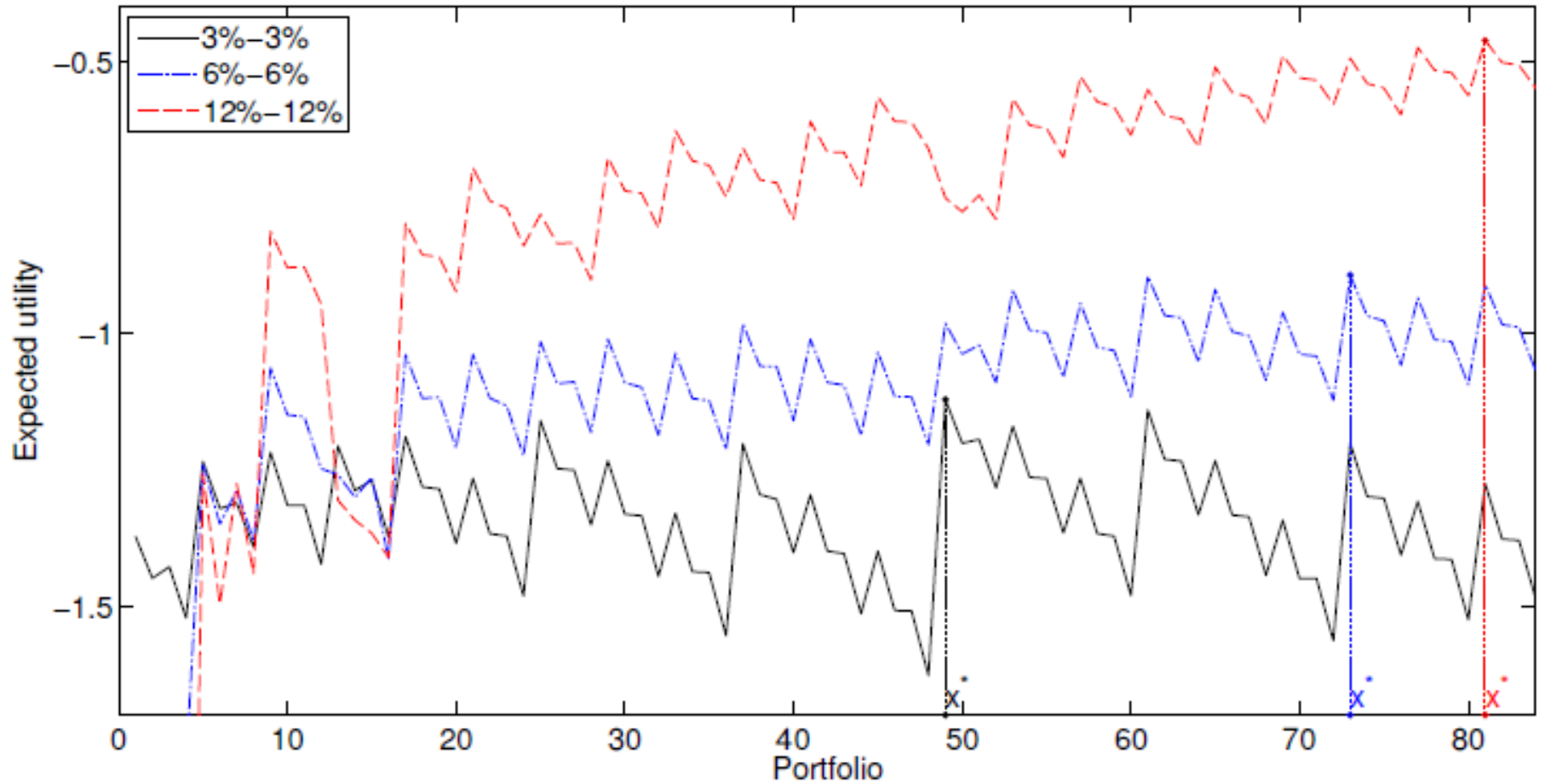## Five types of countermeasures.

- Ticket Inspectors (preventive/recovery).
- Security guards (bouncers), outsourced (preventive).
- Guards (preventive).
- Automatic access doors (preventive).
- Metro employees (preventive),

44

Fare evasion: parameters estimation

Defender

Countermeasures Effectiveness

Deterrent Effects Inspection

Countermeasures Costs

Fraud Costs

Attacker

Number of evaders

Countermeasures Reactions

Costs/Benefits

SECONOMICS
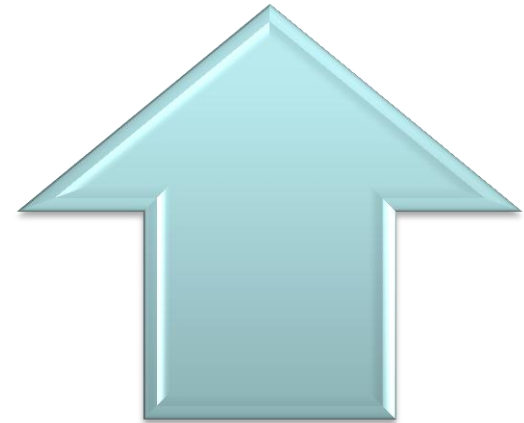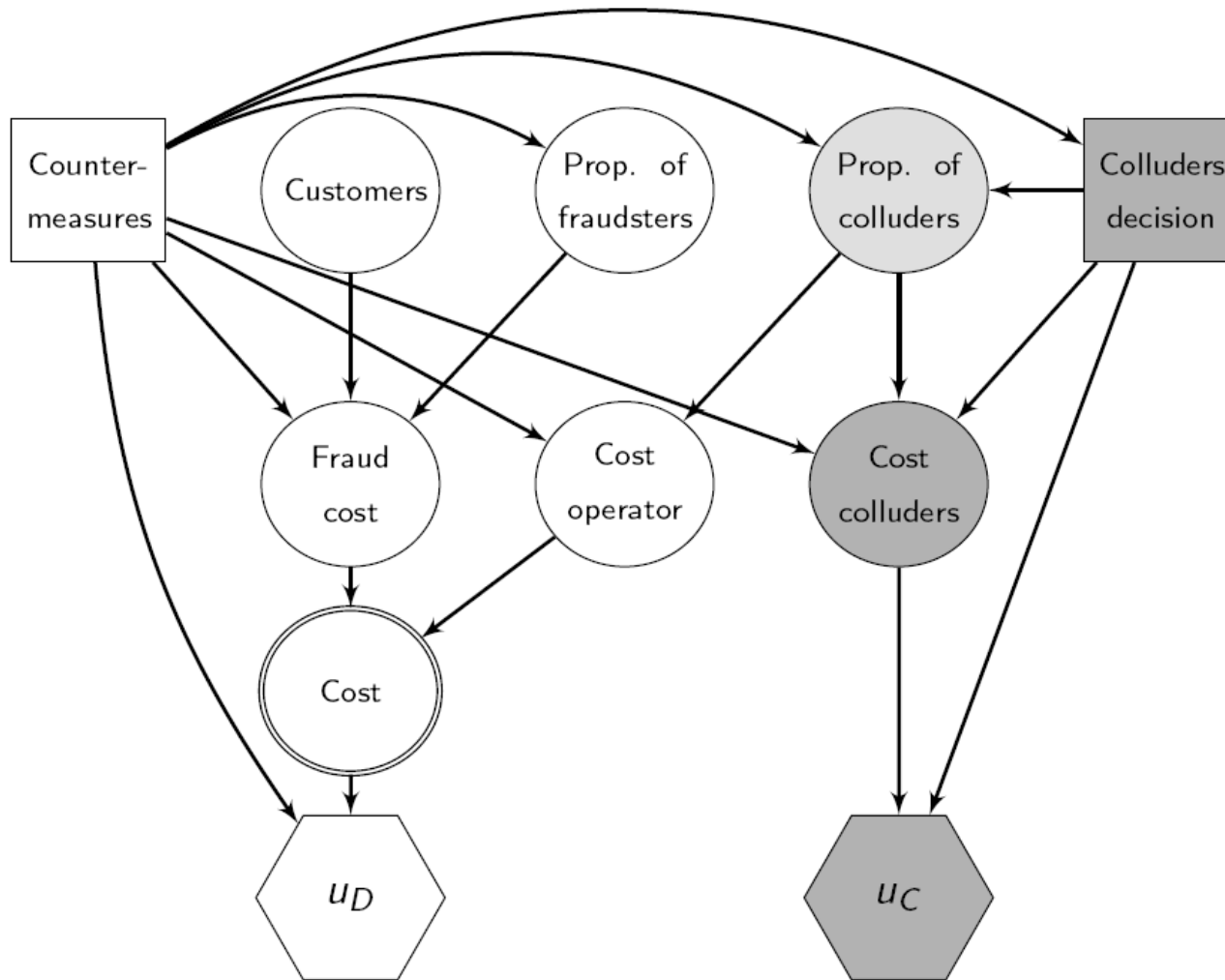
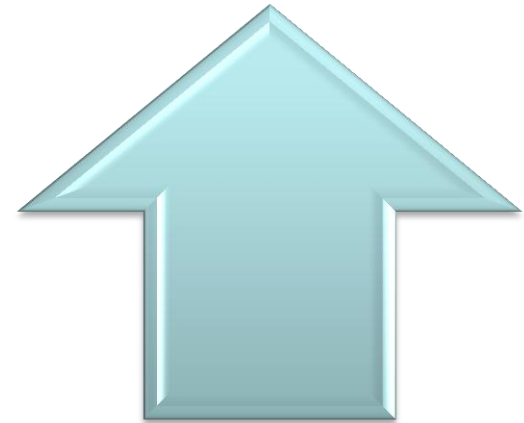| $p_0 + p_r = 0.03, M = 30000$			$p_0 + p_r = 0.06, M = 60000$			$p_0 + p_r = 0.12, M = 120000$		
x	**Inv.**	$\psi(x)$	x	**Inv.**	$\psi(x)$	x	**Inv.**	$\psi(x)$
$(1,0,0,0,0)$	50000	-1.1209	$(1,2,0,0,0)$	100000	-0.89254	$(1,3,0,0,0)$	125000	-0.46182
$(1,0,0,0,0)$	50000	-1.1209	$(1,0,0,0,0)$	50000	-0.98088	$(1,0,0,0,0)$	50000	-0.75091
$(0,3,0,0,0)$	75000	-1.202	$(0,3,0,0,0)$	75000	-0.98208	$(0,3,0,0,0)$	75000	-0.65913
$(0,0,2,0,0)$	60000	-1.2178	$(0,0,2,0,0)$	60000	-1.0626	$(0,0,2,0,0)$	60000	-0.81249
$(0,0,0,1,0)$	15000	-1.428	$(0,0,0,1,0)$	15000	-1.8153	$(0,0,0,1,0)$	15000	-3.5197
$(0,0,0,0,1)$	15000	-1.4488	$(0,0,0,0,1)$	15000	-2.0988	$(0,0,0,0,1)$	15000	-4.1946
$(1,2,1,1,0)$	145000	-1.4142	$(1,2,1,1,0)$	145000	-1.0146	$(1,2,1,1,0)$	145000	-0.52105
$(1,1,2,1,1)$	150000	-1.5636	$(1,1,2,1,1)$	150000	-1.1223	$(1,1,2,1,1)$	150000	-0.5796
$(1,1,2,1,0)$	150000	-1.4494	$(1,1,2,1,0)$	150000	-1.0413	$(1,1,2,1,0)$	150000	-0.53466
$(0,3,2,1,1)$	150000	-1.627	$(0,3,2,1,1)$	150000	-1.2037	$(0,3,2,1,1)$	150000	-0.66057
$(0,3,2,1,0)$	150000	-1.5091	$(0,3,2,1,0)$	150000	-1.1163	$(0,3,2,1,0)$	150000	-0.61212

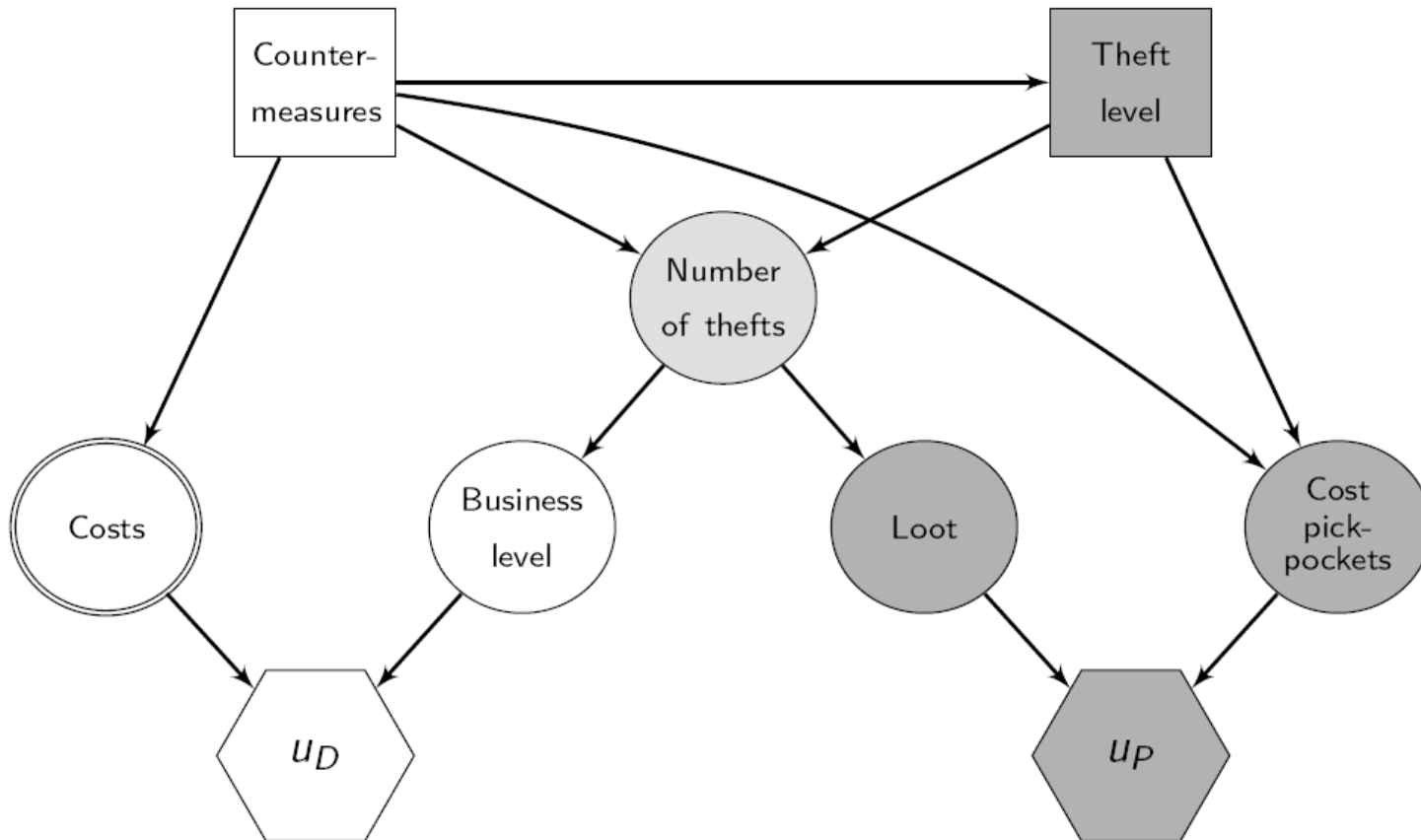SECONOMICS
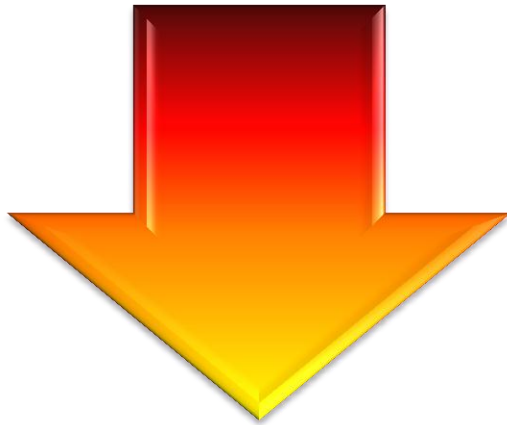
Pickpockets, organized group (2-4 members)

- Attempt t thefts during relevant planning period.
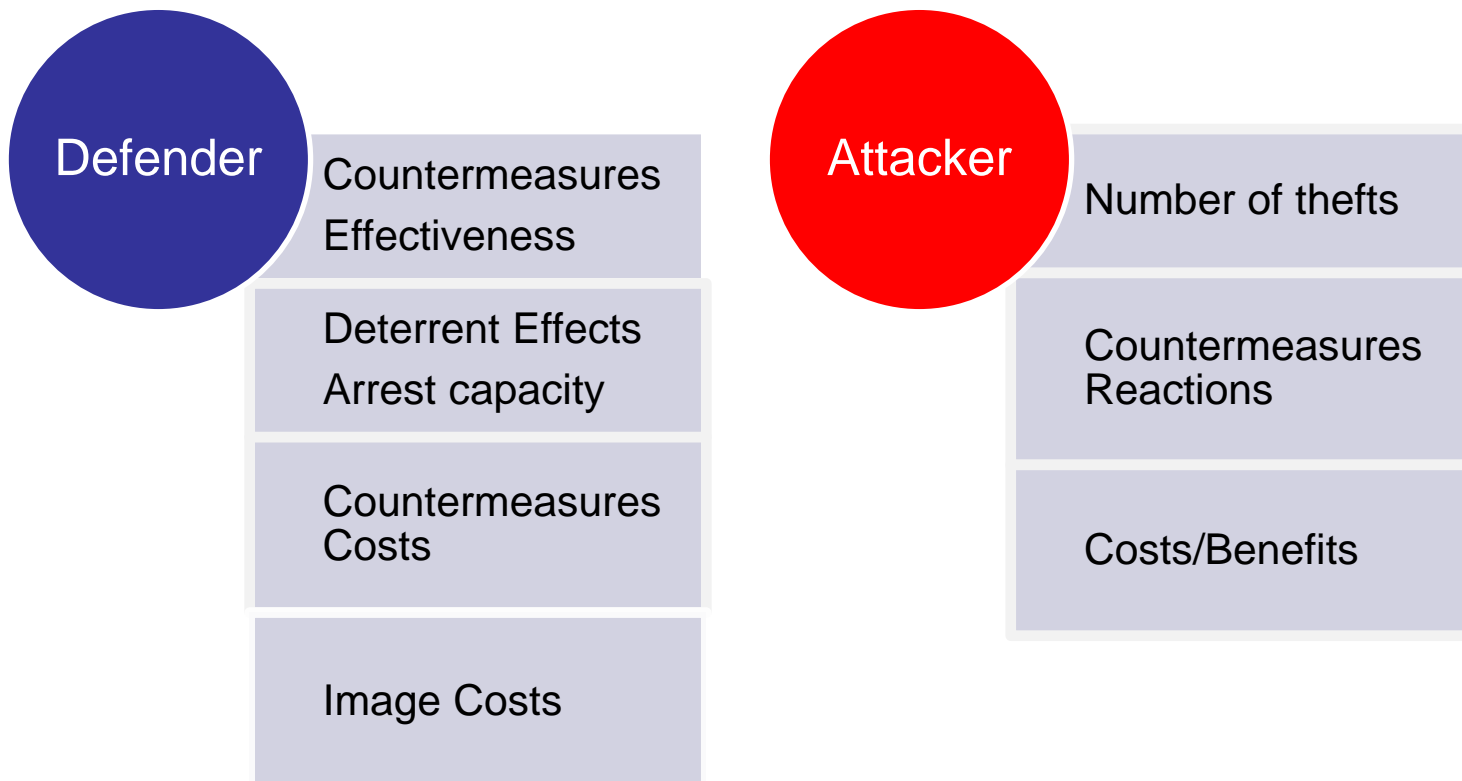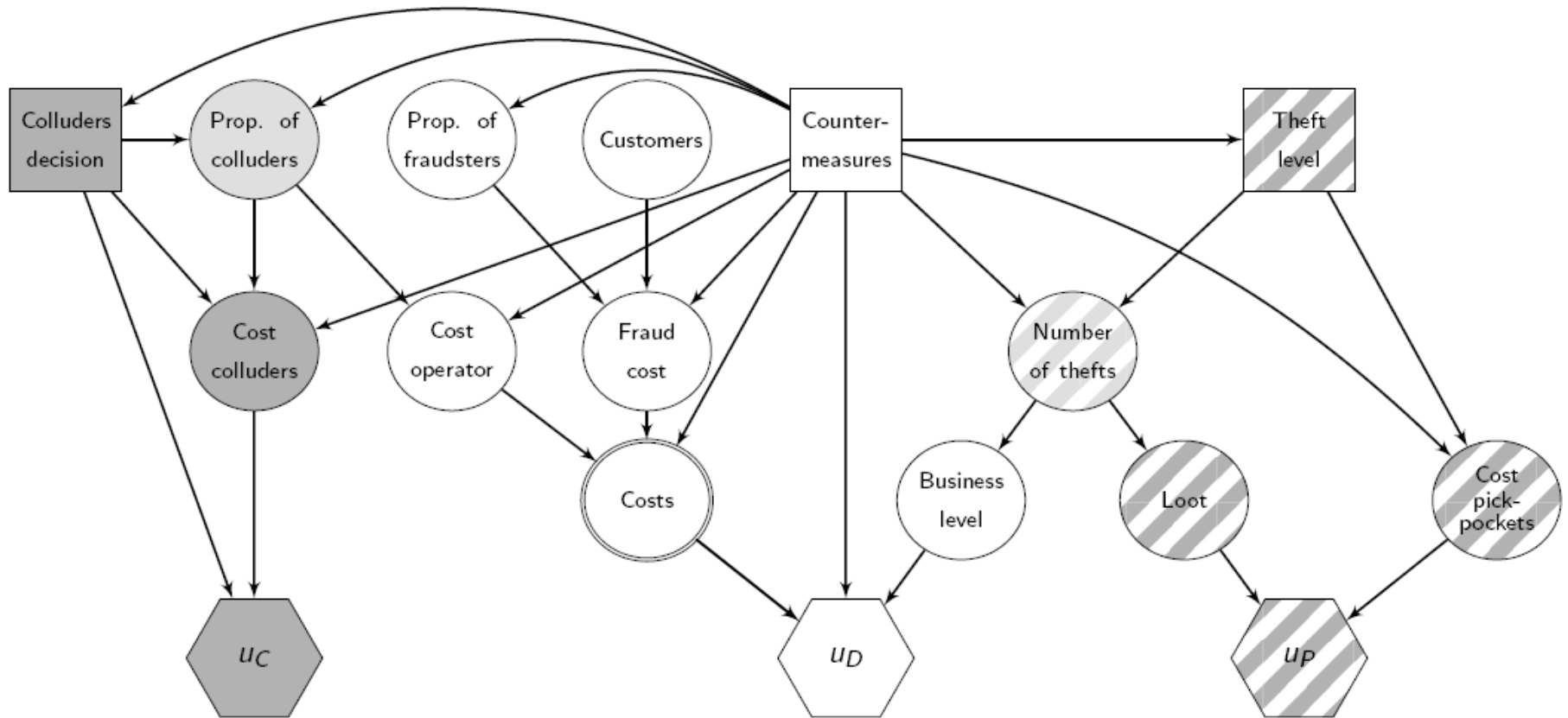- Impact on security and image costs.
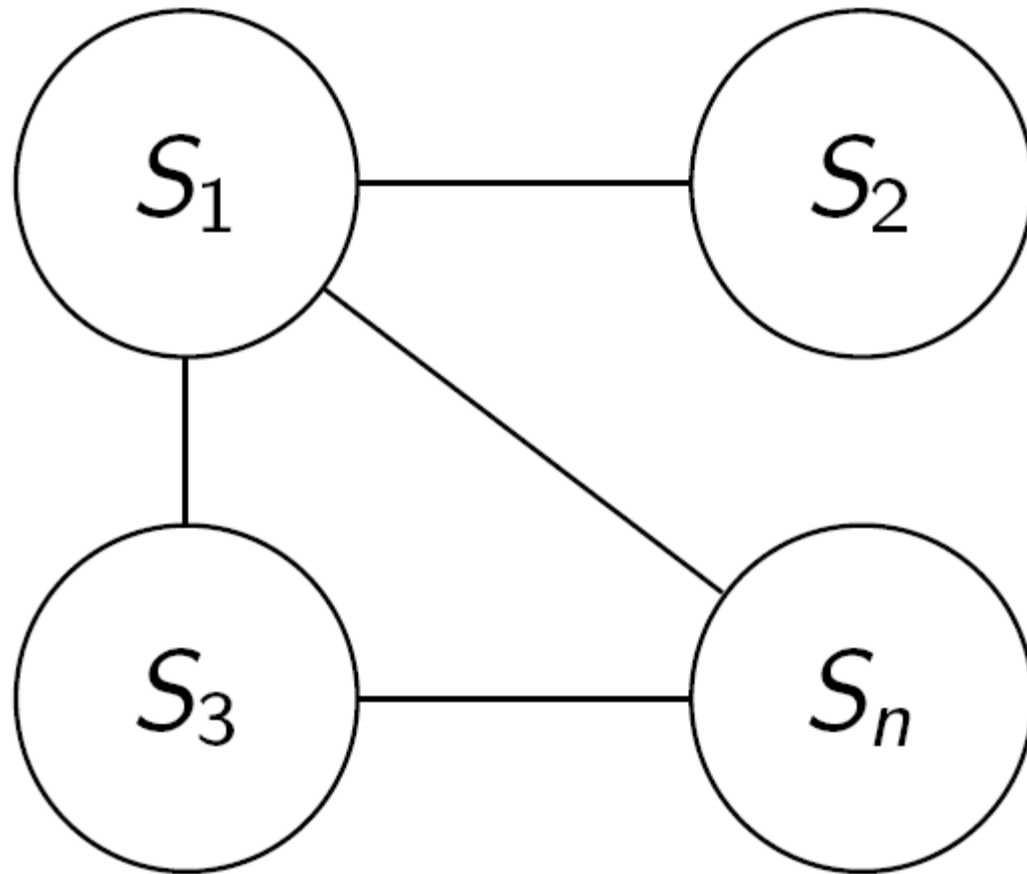
Four types of countermeasures.

- Patrols (guard + dog). Preventive/recovery.
- Cameras. Preventive.
- Guards (shared with fare evasion). Preventive/recovery.
- Public awareness plans. Preventive.

48

SECONOMICS

SECONOMICS

Defender

Countermeasures Effectiveness

Deterrent Effects
Arrest capacity

Countermeasures Costs

Image Costs

Attacker

Number of thefts

Countermeasures Reactions

Costs/Benefits

5.- Open Discussion

SECONOMICS

Future & Emerging threats

- Cybersecurity?

- Displeasure & Fraud?

- Metal Theft?

- Laser-pointer attacks?

- New technologies issues?

- Others?

Pan European coordination (Cross-border threats)

- Graffiti & Pickpocketing?

- Others?

Many thanks for your attention!!